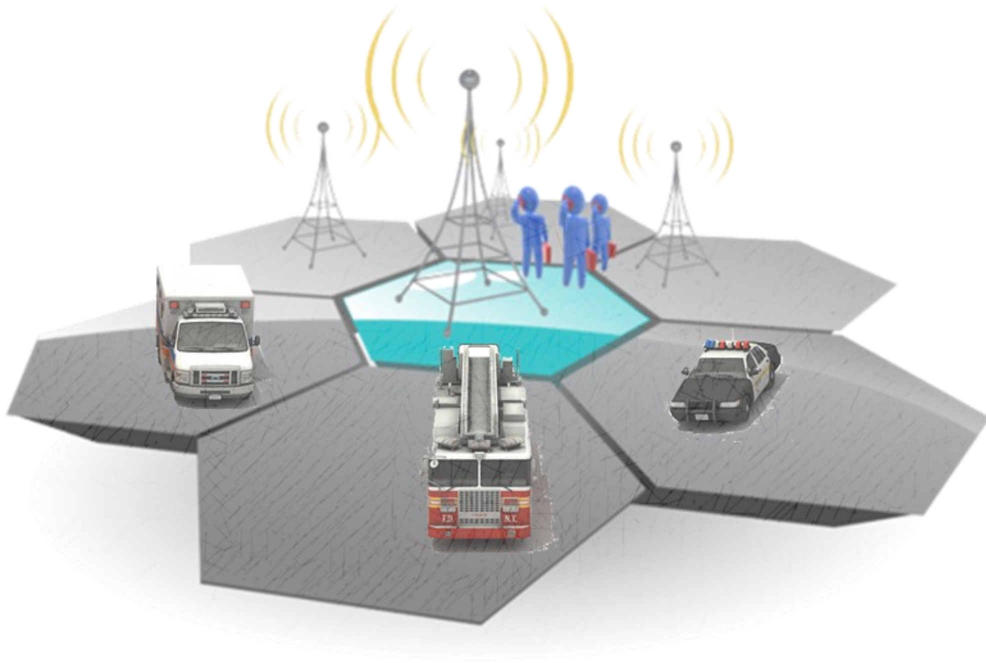
Asociación ITEM
Instituto de Tecnologías
en Emergencias



Interoperabilidad entre las agencias de Emergencias

ANÁLISIS DE ALTO NIVEL.

02/06/2022

CÓDIGO DOCUMENTO: 20220602-1 V1

Contenido

Autores:

- Miguel Alcalde
- Pilar García
- …

Equipo de Revisión

- …
- …

Fecha de la primera edición: 1 Julio de 2022

1 Introducción

1.1 ¿Quiénes somos?

ITEM es una asociación sin ánimo de lucro, registrada en el Ministerio de Interior, entre cuyos fines figura la difusión de información realtiva a sistemas TIC que pudieran ser de interés para los Servicios de Emergencia: Policía, Bomberos, SEM, Protección Civil y UME.

ITEM está compuesta por profesionales del sector, ya sea operativos como tecnólogos, que dedican parte de su tiempo a analizar y proponer el empleo de las tecnologías para respaldar a los servicios de emergencia en su misión.

> "ITEM difunde información sobre sistemas TIC aplicables a los servicios de emergencias".

Para ser socio de ITEM, en el caso de ser funcionario público, no se requiere el pago de ninguna cuota. Tan solo enviarnos un correo donde manifieste su interés, y a partir de ese momento podrá recibir boletines de noticias, o invitaciones a eventos organizados por ITEM o sus socios.

ITEM nació en 2013, y desde entonces ha celebrado algunos actos públicos, siendo el más notorio el Congreso de Tecnologías en Emergencia (UPM, ETSI de Telecomunicaciones), al que asistieron ponentes internacionales como el CEO de NENA.org, miembros de IACP, y gran parte de la industria del sector.

ITEM detuvo su actividad durante unos años por motivos profesionales de sus componentes, pero hemos decidido volver a animar a la Asociación porque la Pandemia ha puesto sobre la mesa muchas necesidades, y la respuesta a las mismas no puede ser unilateral, sino ponderada por observatorios independientes como ITEM.

- Contacto: Tel: 678539300 - mailto: presidenta@asociacionitem.com
- Datos fiscales: CIF: G86675162
- Dirección: C/Pico de la Maliciosa nº 27, Colmenar Viejo, Madrid. España

1.2 Porqué ITEM

Se propone la contratación de este servicio a ITEM, que como asociación goza de la imparcialidad de una Organización sin Ánimo de Lucro, y que cuenta con colaboradores de probada experiencia en este tipo de proyectos, ya sean profesionales de las emergencias en su doble actividad como formadores –

asesores, o consultores TIC que a nombre propio dedican parte de su tiempo a esta actividad en parte altruista.

El dinero recibido servirá para apoyar los fines de la Asociación, y para compensar económicamente a los colaboradores que participen en estas tareas.

ITEM cuenta con socios colaboradores con experiencia en trabajos de consultoría en estudios de viabilidad de soluciones y preparación de Pliegos de Prescripciones Técnicas, como por ejemplo:

- Ingenieros Informáticos
- Ingenieros Telecomunicaciones
- Tecnicos expertos en Planes de Emergencia y Autoprotección
- Directores de Seguridad expertos en Planes de Seguridad
- Policías, Bomberos, Técnicos en Emergencias Extrahospitalarias, y Técnicos de Protección Civil.

1.2.1 Capacidad y voluntad de servicio

En caso de ser elegida nuestra propuesta, estamos en disposición de ofrecer al CLIENTE los siguientes servicios:

- Analizar la mejor alternativa presentada
- Realizar el seguimiento y ejecución de la oferta ganadora.

2 Glosario

A continuación se detalla el glosario de los principales términos usados en este documento. Son definiciones basadas en las especificaciones de sus propietarios, o fruto de la experiencia y conocimiento de los autores de este documento. Pretenden aclarar no solo el significado sino su relación con el objeto del documento.

- **112** : La Comisión Europea considera el número 112 como uno de los instrumentos claves para la libre circulación de ciudadanos dentro de la UE. Este es el motivo por el que en 1991 se creó el número 112, y fue introduciéndose progresivamente en todos los países de la UE cómo único número a través del cual se puede contactar con los servicios sanitarios, bomberos y policía. Mientras en EE.UU. solo existe el **911** para llamar a cualquier servicio de emergencia, en España seguimos teniendo números incluso de 9 cifras para reclamar la intervención de policías locales, y al no existir integración telemática entre los servicios de emergencia, el llamante ha de repetir sus datos a cada operador al que se traspasa su llamada, incrementando la demora para despachar los recursos necesarios.
- **Agencia** u Organización pública de Emergencias: Policía, Bomberos, SEM, P. Civil, …
- **ANI/ALI**: ANI (Identificación de número automático) es el número de teléfono del llamante al PSAP. ALI (Identificación automática de ubicación) es el detalle de la ubicación (la dirección junto con cualquier detalle como el nombre del edificio, el número de suite, el piso o la habitación, etc.). En España esta información es recopilada por la CNMC/Telecomunicaciones y ofrece una base de datos con los abonados o clientes de las Operadoras, ya sean clientes de telefonía fija o móvil. En un municipio, esta base de datos se obtiene del Padrón Municipal.
- **API**: es el acrónimo en inglés de "interfaz de programación de aplicaciones", un componente software que ofrece el fabricante de un sistema que permite que otras aplicaciones se comuniquen con él. El motivo por el cual se añadieron API fue el evitar que terceras aplicaciones entraran a modificar la base de datos de esa solución, porque ese procedimiento genera posibles riesgos operativos fatales como por ejemplo:
    - Caída del sistema
    - Ralentizamiento de la ejecución
    - Falta de integridad en los datos
- **BBDD** o bases de datos. Este tipo de aplicación es un sistema de gestión de información diseñado para el archivo y consulta de datos. Se almacenan de forma relacional, estructurada. Hay otros tipo de bases de datos no relacionales, pero no se contemplan en este documento.
- **Command and Command:** Mando y Control. Los sistemas de información militares o civiles para dirigir operaciones o la respuesta a incidentes. Los tipos de centros de mando y control se clasifican por las capacidades que poseen:
    - **C2:** (Command & Control) Mando y Control.

  - **C4RSI:** (Command, Control, Comunications, Computers, Reconnaisance, Surveillance and Intelligence) Mando, Control, Comunicaciones, Computadores, Reconocimiento, Vigilancia e Inteligencia
  - **C4, C5:** En México se emplea este acrónimo para denominar a los centros de coordinación de emergencias (Centro de Control de Comando, Comunicaciones, Cómputo y Calidad). En Chile se denominan CENCO a los centros de coordinación de incidentes policiales de Carabineros de Chile.
- **CAD** o Computer Aid Dispatch, Sistema computerizado de ayuda al despacho. Se trata de un tipo de solución aplicable a los procesos de recepción de llamada, y asignación de incidentes a recursos (agencias, recursos virtuales, o recursos físicos). Es una solución procedente de los sistemas militares de Mando y Control (Command & Control). En España o América se encuentran aplicados a centros de Coordinación de Emergencias o PSAP que reciben llamadas dirigidas a los números cortos 112 (o 911, 123, 133, 091, 062, 061, 092, …)
- **CiberSOC**: CyberSecurity Operation Center, o centro de operaciones de Ciberseguridad, es un centro de mando para los equipos de ciberseguridad de una organización. Su responsabilidad es supervisar y proteger la tecnología, la Red, los servidores, las aplicaciones y el hardware. No tiene nada que ver con la Seguridad Física gestionada por el responsable de Seguridad de la organización, si bien deberían estar integradas ambas organizaciones bajo un mismo mando, puesto que un ciberataque no se limita a poner salvapantallas poco decorosos, sino que provoca daños físicos. La integración de ambos mundos, el físico y el ciber, la gestión multidominio es un terreno aún no explorado en detalle.
- **COP** o Common Operational Picture, o Imagen Operativa Común: Término en idioma inglés que define el sistema de información que aglutina toda la información requerida, presentándola de manera intuitiva al usuario para que este pueda tomar decisiones correctas. Es un término muy usado en el sector Militar, pero su traslación a la Policía es directo, ya que un Sistema de Gestión Policial nace del concepto de los sistemas informáticos de mando y control militares.
- **COTS** o Commercial Off-The-Shelf: Término en idioma Inglés que define productos listos para usar, que solo precisan de su instalación y configuración, sin ser necesarios desarrollos ni integraciones complejas. Está relacionado con otro término como "Plug and Play", instalar y usar. Este tipo de productos contienen una funcionalidad determinada, y el usuario debe adecuarse a ella. En la industria informática existe la tendencia de poder construir soluciones complejas a partir de productos COTS, porque son soluciones más económicas que desarrollos a medida.
- **CRA**: Central Receptora de Alarmas: Puede ser un sistema TIC que dispara alarmas en caso de detectar la vulneración del perímetro físico de una instalación, o una sala con operadores que disponen de un sistema informático, a modo de PSAP, que permite comprender el motivo de la alarma mediante video vigilancia, y despachar a los recursos que dictamine el protocolo correspondiente al tipo de alarma.
- **DGT**: Dirección General de Tráfico. Es el organismo del Estado que gestiona la principal base de datos sobre vehículos y propietarios. La DGT proporciona datos de los vehículos o personas a

partir de sus matrículas o DNI. De esta manera es posible conocer si un vehículo o su propietario tiene algún interés policial.

- **EAI**: Enterprise Aplication Integration. Se trata de un sistema informático diseñado específicamente para integrar, permitir y orquestar el intercambio de información entre aplicaciones. Estos sistemas facilitan herramientas para definir los lenguajes de intercambio, controlar las transacciones, aplicar procesos de transformación de datos, etc. Muchos CAD COTS incluyen este tipo de sistemas como "Bus de Interoperabilidad", aunque también es verdad que algunos fabricantes venden la capacidad de agregar servicios web mediante programación como si tuvieran realmente un EAI. Algunos productos de este tipo usados en sistemas de emergencia son Microsoft BizzTalk o Tibco.
- **EENA**: European Emergency Number Association (www.eena.org). Es una asociación privada europea que ejerce de asesor en la Comisión Europea, a partir de la directiva sobre el fomento del número único 112 para todos los países que forman parte del Parlamento europeo. Elabora recomendaciones y buenas prácticas para los centros 112 principalmente, a través de sus comités de análisis y diseño.
- **Entidades**: En este ámbito el término entidad se refiere a los seres, objetos o lugares que pueden formar parte de un incidente:
  - Personas
  - Animales
  - Vehículos
  - Empresas u Organismos
  - Domicilios
  - Lugares
  - Números de teléfono
  - Direcciones de Email
  - Perfiles de RRSS
  - Números de cuentas corrientes o tarjetas bancarias
  - Etc.
- **GIS** o Sistema de gestión de información geográfica, diseñado para mostrar mapas e información georeferenciada. Dentro de un sistema CAD existe una vista GIS porque permite comprender el incidente respecto a la ubicación donde sucede, y porque para ciertas personas resulta más fácil gestionar los sucesos en la vista sobre el mapa que no a través de formularios. En la vista GIS de un CAD suelen existir las siguientes funcionalidades mínimas:
  - Ubicar el incidente en su posición física
  - Visualizar y gestionar los recursos propios (despachar, comunicar, …), y visualizar al menos a los de terceras agencias que intervienen en un incidente común.
  - Añadir objetos sobre el mapa para su posterior interrelación con otros datos:
    - Zonas peligrosas
    - Infraestructuras críticas en caso de incidentes
    - Hidrantes y otros elementos desplegados que colaboran en las emergencias

        - Nivel del tráfico obtenido de terceras partes
    - Cargar capas de información de manera dinámica (ráster(imagen), vectorial o puntos de interés) que se consideren oportunas para comprender los sucesos. Por ejemplo capas procedentes de simuladores de incendios o inundaciones.
- **HIS** (Hospital Information Systems): sistema informático para la gestión integral de un hospital. En este tipo de aplicaciones se gestiona el Historial Clínico de un paciente, por lo que resulta necesario poder disponer de él en caso de tener que atenderle en una urgencia extrahospitalaria: grupo sanguíneo, alergias, patologías conocidas, etc., son informaciones críticas. También proporciona información sobre las camas disponibles, que ayudan a la gestión logística del traslado de los heridos. Los sistemas HIS de diferentes hospitales hablan usando el protocolo HL7.
- **HL7**: es un conjunto de estándares basados en XML para facilitar el intercambio electrónico de información clínica.
- **IA** o Inteligencia Artificial. A fecha de redactar este documento, son algoritmos basados en redes neuronales, estadísticos en definitiva, que son capaces a partir de un aprendizaje de proporcionar resultados a problemas que requerirían muchísimas líneas de programación, o incluso para situaciones donde las posibles soluciones son muy numerosas. Relativo a las cámaras, la IA permite reconocer formas en imágenes. Por ejemplo números de matrículas (OCR), objetos, movimientos, cambios de color, etc. Debido al estado del arte respecto a este tipos de algoritmos, la IA puede ir instalada en las cámaras o en el servidor VMS; sí está en las cámaras la potencia y escalabilidad de la solución es más óptima por ser un proceso distribuido.

  IBM define las redes neuronales de la siguiente forma:
  << Una red neuronal es un modelo simplificado que emula el modo en que el cerebro humano procesa la información: Funciona simultaneando un número elevado de unidades de procesamiento interconectadas que parecen versiones abstractas de neuronas.

  Las unidades de procesamiento se organizan en capas. Hay tres partes normalmente en una red neuronal : una capa de entrada, con unidades que representan los campos de entrada; una o varias capas ocultas; y una capa de salida, con una unidad o unidades que representa el campo o los campos de destino. Las unidades se conectan con fuerzas de conexión variables (o ponderaciones). Los datos de entrada se presentan en la primera capa, y los valores se propagan desde cada neurona hasta cada neurona de la capa siguiente. al final, se envía un resultado desde la capa de salida.

  La red aprende examinando los registros individuales, generando una predicción para cada registro y realizando ajustes a las ponderaciones cuando realiza una predicción incorrecta. Este proceso se repite muchas veces y la red sigue mejorando sus predicciones hasta haber alcanzado uno o varios criterios de parada.

Al principio, todas las ponderaciones son aleatorias y las respuestas que resultan de la red son, posiblemente, disparatadas. La red aprende a través del entrenamiento. Continuamente se presentan a la red ejemplos para los que se conoce el resultado, y las respuestas que proporciona se comparan con los resultados conocidos. La información procedente de esta comparación se pasa hacia atrás a través de la red, cambiando las ponderaciones gradualmente. A medida que progresa el entrenamiento, la red se va haciendo cada vez más precisa en la replicación de resultados conocidos. Una vez entrenada, la red se puede aplicar a casos futuros en los que se desconoce el resultado.>>

- **IAED** o International Academics of Emergency Dispatch. Durante más de 40 años, la IAED ha sido la organización de establecimiento de normas para los servicios de envío y respuesta a emergencias en todo el mundo, y es el principal organismo de expertos en asesoramiento de emergencias. Somos, ante todo, una asociación impulsada por miembros que trabaja para servir al público a través del desarrollo profesional de los asesores de emergencias. Contamos con los principales líderes, especialistas, profesionales y autoridades de la industria. Nuestras diversas juntas y consejos trabajan en nombre de los miembros —y en coordinación con otras organizaciones influyentes de seguridad pública— para asegurar que el sistema integral de respuesta a emergencias sea lo más seguro, rápido, eficaz y actualizado posible.
- **Inteligencia**: Es el proceso por el cual se recopilan datos de un determinado domino, se analizan, y posteriormente se genera una conclusión o propuesta de actuación. También se denomina el Ciclo de la Inteligencia, puesto que es un proceso iterativo, de mejora continua. Mediante la Inteligencia es posible predecir el futuro a partir del análisis del pasado. Permite elaborar preguntas como ¿Qué pasaría si…?. Hay procesos o prácticas específicas en Inteligencia como por ejemplo:
    - **HUMINT**: Inteligencia obtenida de seres humanos.
    - **SIGINT**: Inteligencia obtenida a partir de señales. Dentro de esta disciplina se distinguen:
        - **COMINT**: Sobre las comunicaciones humanas a través de medios tecnológicos.
        - **ELINT**: Sobre el espectro electromagnético, por ejemplo la caracterización de señales de radares.
    - **Económica** o Competitiva: Analiza las relaciones económicas.
    - **IMINT**: Analiza las imágenes.

      OSINT: Inteligencia sobre fuentes abiertas o de dominio público
- **Misión Crítica.** Sistema que cumple una función crítica, indispensable, que debe suceder exitosamente. Un sistema puede considerarse de misión crítica cuando se cumple alguna de las siguientes condiciones:
    - La vida humana o la seguridad está en riesgo
    - La investigación o la información están comprometidas
    - Las partes afectadas están sujetas a costos legales, regulatorios o financieros
    - La reputación se ve afectada negativamente de manera significativa
    - Las funciones y aplicaciones comerciales críticas se ven afectadas

- Se experimenta pérdida de datos o acceso a datos

Es obvio que un sistema de gestión de emergencias como el CAD lo es, y por lo tanto debería seguir unos procedimientos de implementación y de mantenimiento acordes.
Un sistema TIC de misión crítica debería estar diseñado considerando:

- Proporcionar interfaces de administración de aplicativos, sistemas y redes para monitorear, consultar y modificar la información de administración, pudiendo entonces tomar decisiones de mantenimiento preventivo e incluso predictivo.
- Aplicaciones de administración de host que permiten la predicción/correlación de fallas e implementan políticas personalizadas de administración de intercambio en caliente
- Enviar información de configuración a otros bloques funcionales relevantes en el sistema
- Administrar configuraciones de aplicaciones y middleware, incluida la modificación de configuraciones existentes y el aprovisionamiento de nuevas
- Supervisión, y generación de alarmas y notificaciones del sistema.
- Hacer accesibles los registros del sistema para inspección y análisis de posibles fallas del sistema

Una característica exigible a los productos comerciales de misión crítica es que no tengan ningún SPOF (punto simple de fallo conocido), es decir, un componente que si falla, haga caer o deje de estar disponible todo el sistema o gran parte de él.
Es habitual exigir a estos sistemas una disponibilidad del 99,99% del tiempo de operación sin fallos. Para ello se recurre a:

- Sistema debe soportar herramientas de monitoreo tipo Nagios, a nivel de cada servicio que compone el sistema.
- Servicio SOC 24x7
- Implantación del servidor en modo Alta Disponibilidad, en modo activo/pasivo como redundante.
- Disponer de dos datacenter en caso de caída del primero
- Datacenter de categoría TIER 4 (estándar ANSI/TIA-942)
- Medidas de tolerancia de fallos a todos los niveles, incluido el interfaz de usuario. Muchas aplicaciones sobreviven a fallos, pero el usuario queda desconectado del sistema y genera pérdida de datos. Esto suele suceder en aplicaciones web mal diseñadas, que carecen de “resiliencia” en caso de caída del servidor o de la conexión con el mismo. No tiene sentido que si se corta la comunicación con el servidor por caerse la wifi o darle una patada al latiguillo ethernet, el puesto de trabajo quede inoperativo: El operador debe poder seguir trabajando como si nada hubiera sucedido, y cuando se restaure el servicio, el sistema debe sincronizarse automáticamente.

- **Multiagencia**: Concepto que se refiere a la capacidad de los sistemas informáticos de gestión de emergencias para gestionar incidentes donde se requiere de la participación de varias agencias. Su correcta interpretación sucede cuando el mismo software es capaz de dar servicio

a la sala del PSAP, y a las agencias que colaboran con ella. El software multiagencia debe ser capaz de gestionar protocolos de recepción de llamada (interrogatorio al llamante) que automáticamente identifiquen y encaminen el incidente a las agencias apropiadas, y que posteriormente sean capaces de aplicar los protocolos de despacho y de actuación de cada agencia. Por ejemplo un sistema multiagencia debe ser capaz de incorporar también los protocolos de catalogación del incidente y de actuación de un SEM, que poseen una complejidad de varios órdenes de magnitud superior respecto a los de una agencia de policía local.

- **Multidominio**: Concepto que engloba a diferentes dominios como por ejemplo el mundo físico, el mundo digital. Tradicionalmente en el ambiente militar se refería a la Tierra, Mar y Aire, hoy en día también incluye el mundo cibernético. Para los servicios de emergencia, solo existe un dominio sobre el cual tienen competencia: el físico. Sin embargo, los daños sufridos por los ciberataques a organismos públicos y privados está impulsando la creación de servicios de seguridad públicos destinados a prevenir, detectar, mitigar o evitar los ciberataques. Por ejemplo en España existe el INCIBE, el Comando Conjunto de Ciberdefensa, y diferentes unidades policiales contra el cibercrimen. Se han creado PSAP destinados a las denuncias de ciberdelitos, lo que aumenta el número de teléfonos que un ciudadano debe conocer para poder pedir auxilio.
- **NENA**: National Emergency Number Association (www.nena.org). Es una asociación privada de EE.UU. dedicada al servicio de los operadores de gestión de la demanda (calltakers) y operadores de gestión de los incidentes o avisos (dispatchers). Ofrece formación y certificación profesional a estos agentes de servicios 911, bomberos, SEM o policías. Además patrocina comités dedicados a la mejora de los servicios de emergencia.
- **OASIS**: La Organización para el Avance de Estándares de Información Estructurada es una asociación sin fines de lucro consorcio que trabaja en el desarrollo, la convergencia y la adopción de estándares abiertos para la seguridad cibernética , blockchain , Internet de las Cosas (IoT), gestión de emergencias , computación en la nube , intercambio de datos legales , energía , tecnologías de contenido y otras áreas. EDXL es un protocolo basado en un conjunto de mensajes estándar XML que facilitan el intercambio de información relativa a emergencias entre los diferentes actores que participan en su gestión y resolución. Este protocolo fue desarrollado por la organización Organization for the Advancement of Structured Information Standards (OASIS) y su objetivo es mejorar la velocidad y calidad en el intercambio de información entre diferentes organizaciones. EDXL: contiene la información necesaria por las tareas de encaminamiento y distribución de la mensajería. El principal consumidor de esta parte es la pasarela, que interpretará la información para encaminar y transformar el mensaje según el destino.
    - **CAP**-EDXL (Common Alert Protocol) , es un formato simple pero general para el intercambio de cualquier alertas sobre emergencia y avisos públicos a través de todo tipo de redes. CAP permite una mensaje de advertencia para ser difundido simultáneamente a través de muchos sistemas de alerta diferentes, por lo tanto aumenta la eficacia de la alerta y

simplifica la tarea de alerta. CAP proporciona un formato de mensaje digital abierto y no patentado para todo
tipos de alertas y notificaciones. No aborda ninguna aplicación o telecomunicaciones en particular. El formato CAP es compatible con las técnicas emergentes, como los servicios web, así como formatos existentes, incluida la codificación de mensajes de área específica (SAME) utilizada para los Estados Unidos, Radio Meteorológica de la Administración Nacional Oceánica y Atmosférica (NOAA) y Sistema de Alerta de Emergencia (EAS), al tiempo que ofrece capacidades mejoradas que incluyen:

- Orientación geográfica flexible utilizando formas de latitud/longitud y otros datos geoespaciales representaciones en tres dimensiones;
- Mensajería multilingüe y para múltiples audiencias;
- Tiempos de vigencia y vencimientos escalonados y retrasados;
- Funciones mejoradas de actualización y cancelación de mensajes;
- Soporte de plantillas para enmarcar mensajes de advertencia completos y efectivos;
- Compatible con encriptación digital y capacidad de firma; y,
- Facilidad para imágenes y audio digitales.

Los beneficios clave de CAP incluyen la reducción de costos y de la complejidad operativa al eliminar la necesidad de múltiples interfaces de software personalizadas para las muchas fuentes de alerta y sistemas de difusión involucrados en advertencia de todo peligro. El formato de mensaje CAP se puede convertir hacia y desde los formatos "nativos" de todos tipos de sensores y tecnologías de alerta, formando una base para una tecnología independiente nacional y "internet de advertencia" internacional. El mensaje de alerta CAP también puede ser utilizado por los sistemas de **sensores** como un formato para informar eventos significativos a los sistemas y centros de recolección y análisis.

- **DE**-EDXL: Describe un marco de distribución de mensajes estándar para compartir datos entre sistemas de información de emergencia utilizando el lenguaje de intercambio de datos de emergencia (EDXL) basado en XML. Este formato se puede utilizar en cualquier sistema de transmisión de datos, incluido, entre otros, el enlace SOAP HTTP. permite a una organización "dirigir" el paquete a organizaciones o personas con roles específicos, ubicados en ubicaciones específicas o interesados en palabras clave específicas. La versión 2.0 tiene la capacidad de usar términos definidos por la comunidad local, usa un perfil de Lenguaje de marcado geográfico (GML), sigue las mejores prácticas para las convenciones de nomenclatura, brinda la capacidad de vincular objetos de contenido, admite extensiones y está reorganizado para mayor flexibilidad y reutilización de tipos comunes. Empaqueta y aborda la información de emergencia para una distribución efectiva con una estandarización mejorada y la capacidad de adaptarse a las necesidades del usuario.
- **ESAP**-EDXL (Emergency Services Alerting Protocol): contiene la información de datos de emergencias que son necesarios para la gestión de la emergencia. El protocolo ESAP está encapsulado dentro de la familia de protocolos EDXL de OASIS. Ha sido creada por

Telefónica para mejorar el intercambio de información entre centros coordinadores de emergencias y organismos que disponen de recursos para resolverlas.

- **HAVE**-EDXL: Permite la comunicación de estado de un hospital, sus servicios y sus recursos. Esta información es vital para seleccionar el hospital más adecuado por capacidad y cualificación para tratar a un herido en función de las lesiones sufridas.
- **RS**-EDXL: Describe un conjunto de mensajes estándar para el intercambio de datos entre emergencias y otros sistemas de información que se ocupan de solicitar y proporcionar equipos, suministros, personas y equipos de emergencia. Este formato se puede utilizar en cualquier sistema de transmisión de datos,
- **SITREP**-EDXL: Describe un conjunto de informes y elementos estándar que se pueden usar para compartir datos entre los sistemas de información de emergencia y que brindan información de incidentes para el conocimiento de la situación en la que el comando de incidentes puede basar las decisiones.
- **TEP**- EDXL: intercambio de pacientes de emergencia e información de seguimiento desde el punto de encuentro del paciente hasta la admisión de atención definitiva o la liberación de campo. TEP admite el seguimiento de pacientes en el continuo de atención de los Servicios Médicos de Emergencia (EMS), así como las evacuaciones de hospitales y las transferencias de pacientes, proporcionando información en tiempo real a los socorristas, Gestión de Emergencias, organizaciones coordinadoras y centros de atención en la cadena de atención y transporte.

- **PEMEA**: El fin de la arquitectura PEMEA es permitir al usuario disponer de una aplicación que cumpla con sus necesidades en cuanto a funcionalidad, coste, y usabilidad, incluyendo los preceptivos parámetros de seguridad y privacidad; y proveer una localización precisa y otro tipo de información añadida a los servicios de emergencia en caso de necesidad, se encuentre donde se encuentre, en Europa. Es un estándar ETSI (TS 103 478) basándose en recomendaciones de EENA y desarrollado bajo el proyecto H2020 NEXES, que permite la interconexión de Apps de emergencia. Permite a los servicios de emergencia (PSAP) recibir información de la persona que llama y una ubicación precisa para una respuesta de emergencia más rápida y efectiva. Implementa funcionalidades avanzadas como chat, RTT, WebRTC para mejorar la accesibilidad universal e inclusiva.
- **PSAP** o Public-safety answering point: Centros de Coordinación de Emergencias, generalmente multiagencia, que atienden llamadas solicitando rescates o comunicando incidentes, y coordinan la respuesta de los servicios de emergencia.
- **PSIM**: Acrónimo de Physical Security Information Management (gestión de la información de la seguridad física). Se trata de una plataforma software capaz de integrar diferentes subsistemas de hardware y mostrar la información que proporcionan de forma centralizada a través de una interfaz común. Mediante asociaciones lógicas, el usuario puede recibir toda la información del sistema (control de accesos, CCTV, sistemas de intrusión…) de forma unificada, lo que le permitirá preestablecer protocolos de actuación. Gracias a la integración de elementos de seguridad con datos de otras plataformas (ERP, BMS…) podemos obtener una herramienta que

eleve el nivel de la gestión de seguridad hasta la excelencia. Para ello es fundamental que el PSIM guíe al operador en un flujo de actuaciones que se definen con anterioridad y que variarán en función de factores como el tipo de alarma, zona, horario, etc. Esta configuración previa es vital para garantizar tanto la eficacia como la trazabilidad y el análisis de los procesos que permiten la mejora continua.

¿Es un PSIM una alternativa a un CAD?: El único elemento que determina su elección es la entidad a proteger. Cuando son las personas, el sistema debe ser siempre un CAD. En el caso de un aeropuerto o una infraestructura ferroviaria, donde existen múltiples elementos industriales como plantas de energía, escaleras mecánicas, etc., la decisión óptima consiste en integrar un CAD con un PSIM, para aprovechar lo mejor de cada uno de ellos. El PSIM para el CAD entonces se convierte en un "sensor" que alertará al CAD en caso de que los mecanismos puedan afectar a la seguridad de las personas.
Usar un PSIM para proteger personas es tan aberrante como usar una herramienta de **ticketing** como Remedy. Sí, aparentemente realizan una función similar, pero los procedimientos para determinar el tipo de incidente y rescatar a las víctimas no contemplan los requisitos que forman parte consustancial de un CAD.

- **RAMS**: Los criterios o parámetros de mantenibilidad, disponibilidad, confiabilidad y seguridad, permiten conocer si el sistema sobre los que se aplican estos criterios es adecuado para su función a lo largo de su ciclo de vida. Procede del mantenimiento industrial. Permite optimizar el rendimiento del sistema, minimizar la pérdida de producción debida a fallos, y aplicar modos de mantenimiento (preventivo, predictivo, correctivo).
- **SDK**: siglas del acrónimo ingles que significa kit de desarrollo de software (SDK). Es un conjunto de herramientas proporcionado usualmente por el fabricante de una solución para permitir la creación de nuevas funcionalidades por terceros sin afectar al producto ni a su operación. Suelen emplearse, como las API, para construir integraciones con otros productos.
- **Ticketing**: Las herramientas de ticketing son un sistema de seguimiento de incidencias, que nos ayudan con su gestión y con otras peticiones de servicios. Hasta hace muy poco, los productos y herramientas de ticketing eran exclusivos del back office de las empresas, sin ninguna relación con el cliente. La gestión de incidentes según ITIL es el proceso de adopción del marco para llevarlo a la práctica. Es una manera de garantizar un servicio de TI eficaz para satisfacer las necesidades de los clientes cuando se produce un incidente.
- **TSO** o Tactic Situation Objects. El TSO proporciona la capacidad de intercambiar piezas de información que participan en el COP (o Imagen Operativa Común). El Objeto de Situación Táctica deberá contener al menos la siguiente información; Datos de identificación, Descripción del evento, Descripción de los recursos, y Descripción de las misiones. Está inspirado en la experiencia de los militares. Esto se explica por el hecho de que la interoperabilidad ha sido un problema de larga data en el ámbito militar. En gran parte, esto se debió a las limitaciones de las operaciones entre servicios, pero también a los requisitos de la OTAN para mejorar la

cooperación durante las operaciones conjuntas multinacionales. TSO no está basado en EDXL, pero como puede gestionar información relativa a operaciones de emergencias, se debería usar DE-EDXL como su paquete contenedor.

- **SIEM:** La información sobre ciberseguridad y gestión de eventos informáticos o SIEM (Security Information and Event Management) es un sistema de seguridad que persigue proporcionar a las empresas una respuesta rápida y precisa para detectar y responder ante cualquier amenaza sobre sus sistemas informáticos. Los sistemas SIEM tienen un control total sobre todos los eventos que suceden en la empresa para poder detectar cualquier tendencia o patrón fuera de lo común y así actuar de forma inmediata. SIEM es la evolución de dos tecnologías de seguridad anteriores:
  - Gestión de eventos de seguridad (SEM). Detecta patrones de acceso fuera de lo común en tiempo real.
  - Gestión de información de seguridad (SIM). Centralización de los registros de seguridad para interpretarlos y almacenarlos en tiempo real, facilitando la actuación inmediata.
- **RMS**: Record Management System. Se refiere al sistema usado por una agencia de cualquier tipo para la gestión de sus expedientes (policía administrativa y judicial). Suele estar basado en un producto BPM (Gestión de procesos de negocio). Su adaptación a cada agencia sucede en la definición de cada expediente. En EE.UU. es el FBI quien define los expedientes policiales para todas las policías de este país, ya sea el propio FBI, las estatales o la de los condados. En España los fabricantes de SGP ofrecen un “Todo en uno” que incluye funciones básicas de un CAD, y otras de un ERP sencillo, y que evoluciona conforme a la buena voluntad del fabricante, o mediante desarrollos a medida que incrementan el coste de la solución.
- **Sala 092**: Sala de mando y control de la Policía Local donde se reciben las llamadas del ciudadano, y se coordina la acción policial. En esta sala es donde se necesita en mayor medida la capacidad de conocer lo que sucede en el municipio, y por este motivo es donde se debe disponer de acceso al SVP.
- **Sensor**: Cualquier tipo de dispositivo capaz de reconocer una determinada condición y emitir de manera digital una alerta. Por ejemplo un termómetro, pluviómetro, volumétrico, o una cámara de video vigilancia dotada de IA.
- **SGF** o Sistema de Gestión de Flota, Los sistemas de gestión de flota se centran en conocer, gestionar los vehículos pertenecientes a una organización. Su objetivo es aumentar la eficiencia, la productividad, la disponibilidad, la seguridad, poder acreditar un nivel de servicio a los clientes. Los sistemas de gestión de Flotas se apoyan en sensores que proporcionan información sobre los vehículos: posición, velocidad, combustible remanente, temperatura de la cabina y otros compartimentos, tripulantes presentes, etc. Estos sensores o balizas se comunican con el servidor mediante red de telefonía móvil (2G a 5G), radio o satélite. Las funciones principales son:
  - Seguimiento de vehículos.
  - Notificaciones del estado del vehículo.
  - Rutas

- Comunicación con el conductor.
- Evaluar los comportamientos de conducción.
- Estadísticas de los conductores.
- Control de mercancías.

- **SGP** o Sistema de Gestión Policial. Software diseñado por ciertas empresas españolas para proporcionar a la Policía una herramienta de gestión integral. Las funciones principales son:
  - CAD: Gestión y coordinación de incidentes recibidos del 112 o de llamadas al 092, o por los propios agentes.
  - RMS: Gestión de las labores ordinarias de la Policía Local: Inspecciones, Sanciones, …
  - Gestión del cuerpo policial: Gestión de Cuadrantes, turnos, material, armero, …
  - Informes y estadísticas

  Se debe mencionar que en España va dirigido a la Policía Local, que tiene muchas menos competencias que una policía integral como la Guardia Civil. Estas soluciones son un a modo de CAD + RMS + algunas funciones que podrían decirse de tipo ERP pero en ningún caso comparable a un ERP auténtico como SAP, Dynamics, SAGE, o incluso el económico Odoo.
  No podemos dejar de citar a los esfuerzos de algunas Diputaciones o esforzados policías que han desarrollado sistemas SGP. Estos software de gestión de policía local son propietarios aunque hayan sido desarrollados por entidades públicas, y no admiten que terceros añadan ningún tipo de mejora o personalización. Además, por ser un negocio con un pequeño número de usuarios potenciales, no pueden o quieren dedicar esfuerzos para estar al día en cuanto a las tendencias del mercado tecnológico. La consecuencia es que cualquier integración incluso con sistemas de administración electrónica municipal son traumáticas y costosas. No obstante a día de hoy son una opción viable, y única para pequeños y medianos municipios.
  Si los fabricantes de sistemas CAD, RMS y ERP tuvieran en cuenta la interoperabilidad designada por EENA, NENA, APCO, ENI, y pensaran en el beneficio del cliente final, las alternativas en el mercado serían más diversas y numerosas, pudiendo incluso un pequeño municipio encontrar soluciones ajustadas a su presupuesto.
  Quizás la lectura de este documento pueda ayudar a esas empresas a mejorar su oferta, esta es una de las razones por las que se fundó ITEM.

- **SVP** o Sistema de Video Vigilancia Policial. Se ha elegido este nombre a propósito para diferenciarlo de los sistemas de video vigilancia aplicados a la Seguridad Privada. Es necesario señalar que es desaprovechar a un policía a labores que todavía realiza un vigilante de seguridad, porque se desprecian sus capacidades si se le dedica a mirar imágenes para tratar de descubrir incidentes. Un policía está para analizar informaciones y actuar ante los incidentes. Los incidentes son detectados por las cámaras. Un SVP consiste por lo tanto en los siguientes componentes:
  - Cámaras
    - Cámaras de vídeo inteligentes que detectan eventos
    - Infraestructura de comunicaciones para las cámaras

        - Material de instalación en vía urbana
    - Servidor de video vigilancia
        - Servidor – grabadora de los vídeos
        - Software de gestión de video vigilancia (Video Management System o VMS)
    - Conector con el Sistema de Gestión Policial: Una cámara no es más que un sensor que advierte de un evento, una alarma, por lo que lo sensato es que este conector esté basado en EDXL-CAP. Para visualizar las cámaras basta con una simple llamada vía protocolo RSTS para recibir el streaming en directo de la cámara. No hay excusa para cobrar esas costosas licencias de conexión que ofrecen los proveedores de video vigilancia o de los SGP.
- **TIC**: Tecnologías de la Información y las Comunicaciones. En inglés ICT.
- **UME**: Unidad Militar de Emergencia. Constituida como un ejército o arma más, a parte del Ejército de Tierra, el Ejército del Aire y la Armada. La UME es una agencia estatal, dotada de recursos muy superiores a los disponibles en una región de España, para intervenir cuando los medios locales son insuficientes, o el incidente afecta a más de una región. Sus componentes son militares profesionales, procedentes de cualquier Arma, y reciben una formación permanente para combatir riesgos naturales y tecnológicos. Su capacidad de intervención es preventiva, reactiva y correctiva, es decir, que es capaz de asistir a los heridos, y reconstruir las infraestructuras dañadas. La UME en sus inicios adoptó un sistema informático para la gestión de emergencias consistente en una modificación de un sistema militar de mando y control porque al ser militares quienes decidían, prefirieron elegir un sistema conocido por ellos. Obviamente esos sistemas no están diseñados para colaborar con los sistemas CAD que usan las agencias convencionales de emergencias. Incluso nos podríamos atrever a decir que al no ser misiones militares sino de emergencias, lo lógico es que la UME usara un CAD corriente, a la altura de sus requisitos, pero un software que aporte la experiencia de este sector que lleva atendiendo a SEM, Policías, Bomberos y centros 112 desde los años 80 del siglo pasado y que tenga asegurado el ciclo de vida del producto gracias a una comunidad de usuarios suficientemente amplia que haga viable este negocio.
- **VMS** o Video Management System. Software diseñado a propósito para gestionar las cámaras:
    - Configurar las cámaras
    - Controlar la visión de las mismas
    - Recopilar los vídeos a modo de un sistema de gestión de contenidos.
    - Presentar los eventos detectados por la inteligencia de las cámaras, como por ejemplo lectura de matrículas.
    - Facilitar la búsqueda, y extracción de videos por diversos criterios como la cámara, momento, evento detectado, etc.
- **WIFI**: Es el nombre de la tecnología de comunicaciones inalámbricas entre dispositivos electrónicos según la norma IEEE 802.11b. En lo único que se diferencia una red wifi de una red Ethernet por cable o fibra es en cómo se transmiten las tramas o paquetes de datos; el resto es idéntico.

3 Referencias

Se añaden a continuación enlaces a las fuentes usadas para elaborar este documento, o para ilustrar ciertas opiniones de los autores del documento que pudieran ser controvertidas.

ANI/ALI
https://docbox.etsi.org/stf/archive/stf321_tispan3_ec_emergency_call_location/public/library/nena%20documents/nena%2002-010%20standard%20format%20for%20data%20exchange.pdf

Búsqueda Semántica
https://developer.expert.ai/ui
http://ceur-ws.org/Vol-440/paper3.pdf

CAD2CAD
https://www.govthink.com/2019/05/11-life-saving-benefits-of-cad-to-cad-interoperability/
https://www.police1.com/police-products/police-technology/software/cad/articles/why-cad-to-cad-networks-are-mission-critical-in-emergency-services-SdPKdxGcNvizc2n5/
https://www.centralsquare.com/public-safety/cad/cad2cad
https://apps.dtic.mil/sti/pdfs/AD1123273.pdf
https://www.nist.gov/system/files/documents/2019/06/27/nist.ir_.8255.pdf

ENI
https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio/pae_Normas_tecnicas_de_interoperabilidad.html
https://administracionelectronica.gob.es/pae_Home/dam/jcr:f92d3fda-5aa0-42ab-b665-26ffd92b100d/TECNIMAP_2010_Resumen_sesion_3.pdf

Estándares en el sector de las Emergencias:
https://www.w3.org/2005/Incubator/eiif/wiki/EMInfoStdsReview#Review_of_Emergency_Management_Information_Standards

HL7
https://www.disrupciontecnologica.com/hl7/

Inteligencia
https://usnwc.libguides.com/c.php?g=494120&p=3381426

Inteligencia Artificial
https://www.ibm.com/docs/es/spss-modeler/SaaS?topic=networks-neural-model

Multidominio
https://usnwc.libguides.com/c.php?g=494120&p=3381426
https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Tercer-Trimestre-2021/Skates-Tercer-Trimestre-2021/
https://www.alhambrait.com/productos/alerta/

NDEX:
https://www.fbi.gov/services/cjis/ndex

OASIS, EDXL y CAP
https://www.oasis-open.org/
http://docs.oasis-open.org/emergency/edxl-de/v2.0/edxl-de-v2.0.html
https://hmong.es/wiki/OASIS_(organization)
https://1library.co/article/integraci%C3%B3n-con-organismos-externos-problemas-principales.y4wr73kq
https://docs.oasis-open.org/emergency/cap/v1.2/pr03/CAP-v1.2-PR03.pdf

Organizaciones que promueven estándares de Emergencias
https://eena.org/knowledge-hub/documents/
https://www.nena.org/page/Standards
https://www.apcointl.org/technology/interoperability/

PMEA:
http://ierd.es/pemea-arquitectura-para-una-app-paneuropea-de-emergencias/
https://eena.org/knowledge-hub/press-releases/pemea-architecture-document-published-by-eena-technical-committee/
https://eena.org/knowledge-hub/documents/pemea-protocol-procedures-specification/
https://www.etsi.org/deliver/etsi_ts/103400_103499/103478/01.01.01_60/ts_103478v010101p.pdf

Protocolos
https://www.emergencydispatch.org/what-we-do/emergency-priority-dispatch-system
https://prioritydispatch.net/discover_proqa/

PSIM
https://elblogdesecuritas.es/tecnologia/psim-de-la-simple-gestion-a-la-excelencia-en-la-seguridad/

PSIM vs CAD:
https://www.youtube.com/watch?v=TI_u_z4-5Zk
https://www.asmag.com/showpost/15522.aspx

SIEM:
https://www.ambit-bst.com/blog/qu%C3%A9-significa-siem-y-c%C3%B3mo-funciona
https://pandorafms.com/blog/es/que-es-siem/

Sistemas de misión Crítica
https://apps.dtic.mil/sti/pdfs/ADA627258.pdf

TSO
https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017R2196&from=EN
https://www.oasis-open.org/committees/download.php/42411/CWA_15931-1

UME
https://administracionelectronica.gob.es/pae_Home/dam/jcr:f92d3fda-5aa0-42ab-b665-26ffd92b100d/TECNIMAP_2010_Resumen_sesion_3.pdf

4 Resumen

Este documento analiza, diseña y propone métodos ya existentes, probados, fiables para integrar de manera telemática los diferentes sistemas usados por servicios de emergencia entre otros similares, y con otros sistemas que aportan información valiosa para las agencias responsables de la seguridad de los ciudadanos:

- Centros de Coordinación de Emergencia, que atienden llamadas al número corto 112
- Servicios de Emergencia Médicos (SEM) o SAMU (Servicios de Asistencia Médica de Urgencias), popularmente denominados "ambulancias", que realizan la atención extrahospitalaria de los heridos en un incidente.
- Servicio de Prevención, Extinción de Incendios y Salvamento (SEPEIS), o Bomberos
- Policías, Locales o Municipales, regionales o nacionales.
- Agrupaciones de Protección Civil
- U.M.E: Unidad Militar de Emergencias.
- CiberSOC: Servicio de ciberseguridad encargado de proteger una jurisdicción administrativa o territorial.

El **objetivo** de este documento es promover el **empleo de estándares** para compartir información entre los sistemas informáticos de los servicios de Emergencias, para lograr los siguientes **beneficios** :

- **Mejorar** los **tiempos de respuesta** de las agencias para detectar y responder a un incidente.
- **Permitir** generar **inteligencia** a partir de la información de cualquier **dominio** donde la agencia tenga **jurisdicción**.
- **Minimizar** los **costes** de integración entre los sistemas
- **Minimizar** los **plazos** de puesta en marcha de sistemas informáticos que deban "hablar" con los existentes.
- Facilitar la **Mantenibilidad** mediante la obtención de indicadores RAMS sobre los sistemas informáticos de las agencias, facilitando el reemplazo de los sistemas obsoletos por otros nuevos, buscando el "instalar y usar"'
- Evitar migraciones de datos al reemplazar un sistema.
- Favorecer la **Escalabilidad** de los sistemas al no depender de ellos mismos el incremento de la funcionalidad buscada.
- Delimitar de manera nítida la **responsabilidad en las integraciones**, trasladando al fabricante o implementador de la solución esta tarea a la etapa de construcción de la solución, y no durante la implantación.
- Introducir el concepto **Multi-Dominio,** para Integrar las alertas de **ciberataques** en la seguridad física.
- Mejorar la **industria del sector**, mediante la compartición de este documento de manera gratuita.

La **interoperabilidad** tratada se refiere tanto a sistemas propietarios como de dominio público, así como de fuentes abiertas o propietarias.

5 Introducción

Este documento tiene aplicación válida para cualquier país. No trata aspectos relativos al marco jurídico ni legislativo, sino asuntos relativos a los sistemas tecnológicos usados por las agencias de emergencia y seguridad pública. El documento está personalizado para España, si bien tan solo se realiza como ejemplo o referencia.

En pleno siglo XXI, la comunicación de incidentes a las agencias de despacho, policías, bomberos, SEM o P. Civil, se sigue realizando por teléfono en muchos casos, algunas agencias disponen de un terminal remoto del 112, y muy pocos tienen integración telemática, "machine2machine" entre sus sistemas de información. La comunicación entre centros 112 no se menciona de manera intencionada, al no disponer de información para poder explicar como sucede.

El resultado de esta situación es que no se puede generar Inteligencia de forma rápida y eficaz. Y sin Inteligencia, los sucesos provocados por riesgos naturales o tecnológicos o por los cacos, son difíciles de predecir, conocer y de responder a tiempo.

Aunque en este documento se argumenta tomando como ejemplo a sistemas policiales, todo el contenido puede ser fácilmente extrapolable a cualquier otro de sistema de interés para cualquier agencia.

5.1 Objetivo

Actualmente, cuando una agencia adquiere una solución de Gestión de Emergencias, u otra complementaria, se encuentra con que requiere que esta nueva solución dialogue con las ya existentes para alimentarse o alimentar al sistema en su conjunto.
Se suele requerir que las soluciones dispongan de conectores con los sistemas habituales, o la capacidad de integrarse con ellas. Y se recurre a solicitar a los integradores o fabricantes credenciales que demuestren que las poseen: Los principales retrasos en cualquier tipo de proyecto procede de los problemas que surgen en las integraciones. La siguiente tabla resumen los métodos usados y sus riesgos.

Modo integración / Riesgos	**Motivo**	**Riesgo 1**	**Riesgo 2**	**Riesgo 3**	**Valoración global**
CASO A: Desarrollo a medida	• Aplicación sin SDK ni API	Problemas concurrencia	Entorno de pruebas de los dos	Coste del desarrollo y del	Desaconsejabl e porque:

accediendo a la BBDD	• Fabricante ya no existe • Fabricante no colabora • API o SDK sin documentación	entre las dos aplicaciones	sistemas para comprobar errores.	mantenimiento del conector	• impide el evolutivo de cada aplicación por separado, • puede provocar graves fallos
CASO B: Existe API o SDK	Ninguno de los sistemas a integrar aporta la capacidad de diálogo mediante protocolos abiertos.	Posible coste de formación /Certificación en el API o SDK	Entorno de pruebas de los dos sistemas para comprobar errores.	Coste del mantenimiento del conector	Aumenta los plazos de integración
CASO C: Uso de protocolos de comunicación propietarios	Los responsables de cada producto acuerdan un método a medida para compartir información	Fallo en la integración si una de las dos partes decide finalizar el soporte a ese método	Posible demora porque ambas partes deben llegar a un acuerdo de integración.		No permite sustituir alguna de las dos soluciones sin tener que volver a replantear la integración
CASO D: Uso de protocolos basados en estándares abiertos			Entorno de pruebas no necesario. Es el fabricante quien debe validad en "fabrica" que su sistema es interoperable.		Es la opción más recomendable porque permite al cliente evolucionar sin tener en cuenta las integraciones.

Algunos casos específicos que suelen ocurrir son

- El responsable de la implantación de una de estas soluciones, o el propio fabricante no quiere o no dispone de recursos para atender peticiones para colaborar en integraciones, lo que deja al cliente sin una integración vital para el buen funcionamiento del sistema global.
- El fabricante de una de estas soluciones impone elevados costes de integración, o de certificación-formación para permitir a terceros el uso de sus API o SDK.

Los siguientes gráficos evidencian la situación actual y el motivo de este documento:

CASO A:

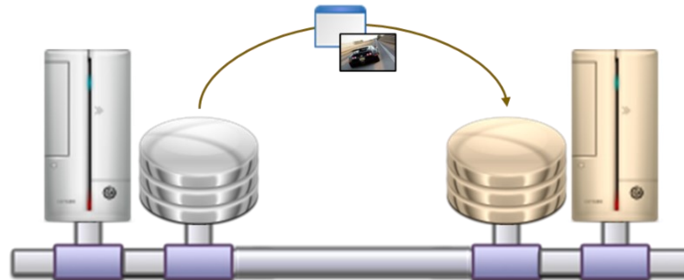


Ilustración 1 Integración nada aconsejable, donde un sistema accede a la base de datos de otro para tomar información que le interesa. Esto puede provocar problemas de concurrencia entre ambos sistemas, corrupción de los datos o caída de alguno de los sistemas.

CASO B

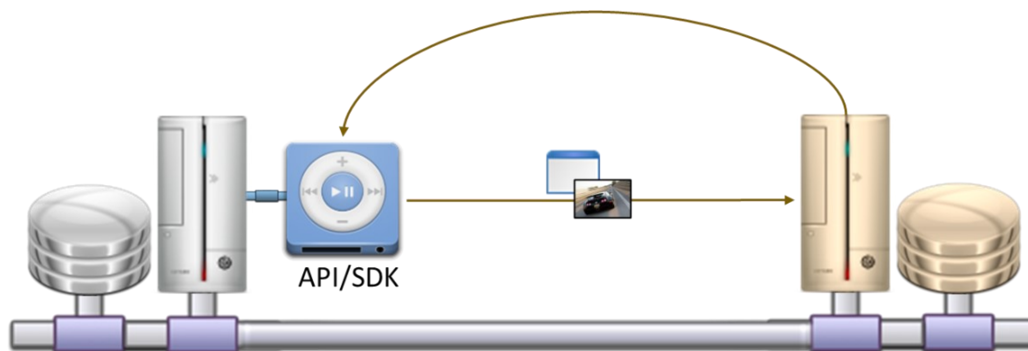


Ilustración 2 Integración habitual entre un VMS y un SGP, donde debe utilizarse un interfaz propietario por parte del otro sistema, lo que requiere finalmente un desarrollo a medida que mantener.

CASO C

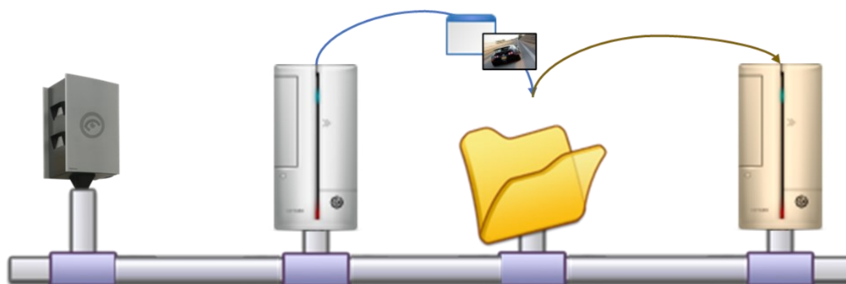


Ilustración 3 Integración entre un Radar de Velocidad y un SGP o de Tramitación de Denuncias

CASO D

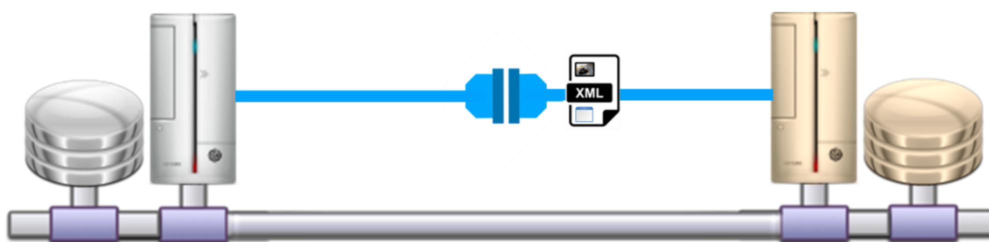


Ilustración 4 Integración mediante protocolos abiertos. Si ambos sistemas disponen de capacidad para dialogar mediante protocolos estándares, en lugar de integración hablamos de "Instalar y usar".

A continuación se expone el mismo asunto desde otro punto de vista:

	Cumple con requisitos de sistemas de Misión Crítica	Riesgos	Ventajas
CASO B	No. Es un modo de acceso que no tiene en cuenta al otro sistema, por lo que carece de protocolo de negociación en las transferencias	Es un método a medida. No está sincronizada la lectura de datos por lo que puede provocar fallos de integridad. Genera un punto de fallo único si ambos sistemas tratan de escribir y leer sobre el mismo registro.	Tradicional
CASO C	Sí. Es asíncrono, soporta redundancia, no genera punto único de fallo	Requiere formación para usar el API, entorno de desarrollo y pruebas, etc. La integración no deja de ser una solución a medida que hay que mantener.	Solución elegante, mantenible.
CASO C	Sí. Es asíncrono, soporta redundancia, no genera punto único de fallo	Es un método "a medida".	Sencillo
CASO D	Sí. Es asíncrono, soporta redundancia, no genera punto único de fallo	Ninguna de las dos aplicaciones necesita conocer a la aplicación con la cual va a compartir información, tan solo conocer el lenguaje de interoperabilidad	Solución elegante que no requiere servicios de mantenimiento puesto que el protocolo abierto y estándar no varía.

La simplicidad del CASO C es lo que induce a proponer el CASO D como óptimo para casi todos los casos. La justificación se basa en casos como por ejemplo la integración de los radares de velocidad con otros sistemas como CAD, RMS o Gestión de la Tramitación de los Expedientes Sancionadores.
En estos casos los fabricantes de Radares o FotoRojo optan por dejar en una carpeta del disco duro compartido o directorio FTP, por cada detección de la violación del límite de velocidad, un fichero con los metadatos, y las fotos requeridas para justificar la sanción.

5.2 USA como ejemplo

El modelo de **interoperabilidad** tecnológica que se está implementando replica en cierto modo a Internet, todos con todos, aunque el FBI es el nodo central que archiva todos los datos del país entre otras capacidades.
Un ejemplo es la base de datos N-DEX que recopila información de todas las agencias de seguridad pública de USA; y que a su vez permite a cualquiera de ellas consultar cualquier dato sobre una entidad (persona, vehículo, domicilio, teléfono, etc). Con este sistema, una policía de un condado puede preguntar si pasó por alguno de los condados vecinos una furgoneta gris, usando lenguaje natural, porque es mucho más eficaz este tipo de motores de búsqueda semántico o “texto libre”, que los puramente relacionales.
Otro que viene al caso es el sistema que implementan agencias policiales o centros 911 para hablar con sus vecinos, no solo para compartir consultas, sino para colaborar en incidentes. Este tipo de sistemas denominado CAD2CAD, permite a un despachador, al agente que gestiona los recursos asignados a un incidente, coordinar también a recursos de otras agencias, o asignar a estas otras agencias incidentes derivados del principal que sus propios recursos sobre el terreno detectan.

5.3 Durango también como ejemplo

La Policía Local de Durango - España, hace uso de las fuentes abiertas (meteorología, etc) para enriquecer su conocimiento del municipio, y así poder reaccionar a tiempo ante la crecida de un rio, o una ola de calor. Estas fuentes desgraciadamente no comparten los datos de manera homogénea, y por eso su empleo es reducido, por los costes que genera su integración.

5.4 Inteligencia

En este documento hablamos de dos “Inteligencias”:

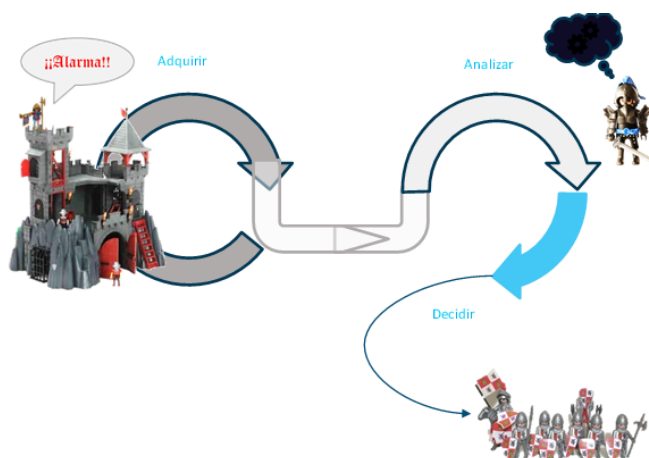
Inteligencia Artificial: Algoritmos capaces de automatizar tareas humanas repetitivas, como por ejemplo búsquedas de información no estructurada (imágenes, voz, vídeo, bases de datos, …). Estos

algoritmos están basados en la supuesta simulación de como actual las redes neuronales. De forma resumida se puede decir que son “Búsquedas Estadísticas”.

Inteligencia: Se puede describir como la capacidad de percibir o inferir información a partir de datos, y retenerla como conocimiento para tomar decisiones. Los sistemas automáticos de tipo “sensor”, como por ejemplo un termómetro o un cinemómetro, son capaces de convertir un dato, en información, de ver un vehículo circulando por una zona, y deducir la velocidad a la que circula.
Los servicios de emergencias necesitan Inteligencia para poder responder a tiempo, y correctamente, por eso el aprovechamiento de cualquier fuente de información que permita comprender lo que sucede es necesaria.

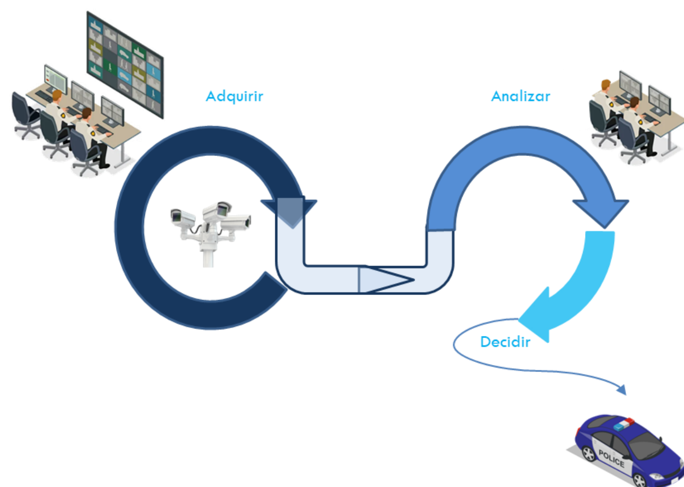
No hay ningún tipo de agencia de emergencias que no vea mejorada su capacidad sin disponer de Inteligencia. Es más, un servicio de emergencias sin inteligencia no sería eficaz. Por eso se requieren múltiples fuentes de información, todos los datos a los que se pueda tener acceso, para poder cumplir su misión. Incluso a aquellos datos que se pudieran considerar de acceso restringido: clasificados, reservados o secretos, porque los servicios de emergencia tienen necesidad de conocerlos.

5.4.1 Inteligencia en la video vigilancia

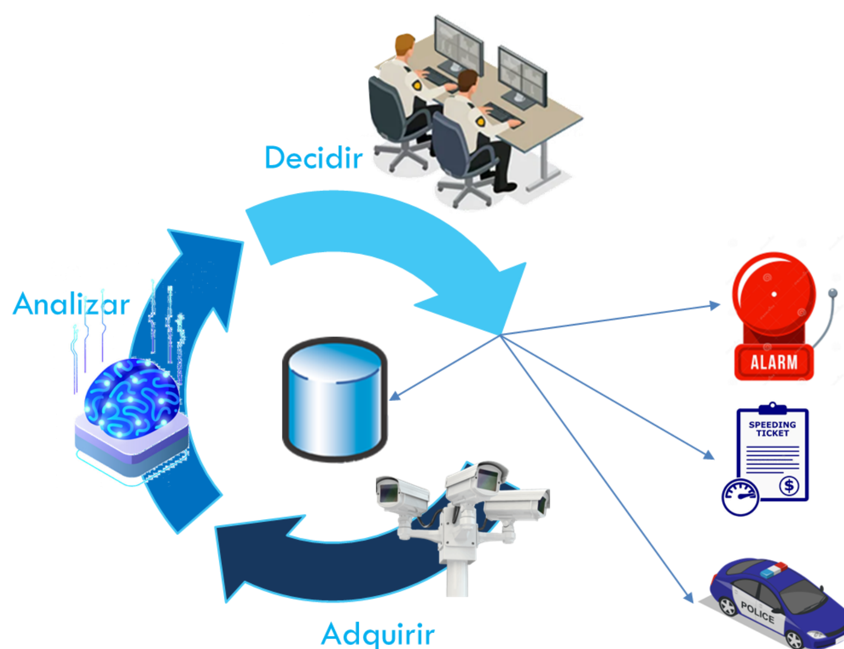


En tiempos no demasiado lejanos, los servicios de seguridad de un castillo disponían de un rol específico relacionado: Los vigilantes, cuya función era y sigue siendo detectar la aproximación de un evento clasificado como de riesgo para el castillo: Una horda de vikingos, las mesnadas del vecino para ultrajar a las hijas del señor del castillo mientras este está ausente peleando contra el moro, un dragón, la subida del caudal del río, o un incendio. Estos vigilantes debían alertar al director de seguridad de la instalación con los medios de comunicación que tuvieran a su disposición: señales acústicas, luminosas, eléctricas, o digitales. Hasta la llegada de las señales digitales, la cantidad de información emitida era muy escasa, por lo que la toma de decisión del responsable de seguridad podía fracasar si no actuaba con prudencia. Esta demora en responder podía ser en sí misma el motivo de las pérdidas de vidas y bienes.

La introducción reciente de sistemas informáticos tipo CAD, manteniendo a los vigilantes, no fue el factor determinante de la mejora en el tiempo de respuesta y eficacia de la actuación, sino las radiocomunicaciones. Por este motivo muchas agencias siguen considerando la radio como su sistema principal. Pero el factor humano, la cantidad de agentes y su capacidad de atención, limita su idoneidad. Por este motivo las salas de video vigilancia sencillas, donde el operador debe estar mirando la pantalla de forma intensiva durante su turno, no son eficaces para detectar eventos: La fatiga y el funcionamiento del cerebro a la hora de interpretar lo que ve, producen fallos en el servicio prestado.



La aplicación de algoritmos de IA en la video vigilancia, la visión artificial, fue uno de los primeros campos donde se desarrolló de forma práctica esta tecnología. También para el reconocimiento óptico de caracteres. Posteriores algoritmos de análisis de imagen permiten detectar la velocidad relativa de los objetos, el número y tipo de los mismos, etc. Gracias a este avance tecnológico y su aplicación a la seguridad, la función del vigilante se ha “transformado digitalmente” o ha sido reemplazada por una cámara inteligente. Esta mejora hace innecesaria la Sala de Video Vigilancia, puesto que es capaz la cámara por sí misma de ofrecer información rica y fiable sobre el evento que ha detectado. Además, esta automatización acelera el ciclo de la Inteligencia, en las fases de recopilación y análisis, dejando al humano que ejerce de despachador, decidir la mejor respuesta



5.5 Inteligencia de las cámaras y sistemas IoT

El desarrollo de la tecnología, de los algoritmos basados en redes neuronales, en "Machine Learning", y "Deep Learning" permiten detectar diferentes tipos de objetos, realizar operaciones lógicas y algebraicas de manera automática y con elevado grado de acierto.
El caso más común es la lectura de matrículas entre soluciones para Policías Locales. No obstante comienzan a aparecer empresas que ofrecen detecciones muy interesantes como:

- Semáforos Foto Rojo: Detectan si un vehículo sobrepasa la línea transversal del semáforo estando este en rojo, en cuyo caso toman varias fotografías del hecho para documentar la infracción. En algunos casos también capturan la matrícula del vehículo para poder emitir el boletín de la denuncia sin recurrir a un agente excepto para su revisión.
- Foto Stop: Similar al "Foto Rojo".
- Etc.

Algunos sistemas VMS avanzados permiten crear funciones adicionales a las que aportan las cámaras, como por ejemplo unir varias cámaras para calcular velocidades medias en un trayecto, considerar otros sensores como un micrófono, sensores, u otras cámaras, para por ejemplo proponer una alarma por conducción deportiva en caso de que un vehículo derrape en una rotonda.

En el siguiente gráfico se enumeran algunas de las capacidades de las cámaras inteligentes respecto a la detección de alarmas, junto con diferentes dispositivos dotados de cámaras que podrían ser de interés para los servicios de emergencia:



Sistemas IoT o sensores en general que son capaces de contar el paso de vehículos, apertura de puertas, volumétricos, termómetros, sismómetros, pluviómetros, … propios o procedentes de fuentes abiertas, son fuente de alertas que proporcionan inteligencia a los sistemas CAD. En Argentina se implementó un

6 Situación Actual

6.1 Sistemas Informáticos para la gestión de las agencias de emergencias

Se enumeran de forma somera los principales sistemas de información implantados a fecha de redactar este documento. La no mención a cierto tipo de aplicaciones se hace para enfatizar el objetivo del documento, porque son confidenciales, o por desconocimiento de los autores.

6.1.1 Policías Integrales

Las policías nacionales y regionales con plenas competencias en materia criminal, gracias a los grandes presupuestos de los que disponen, han podido construir aplicaciones específicas para cada función que realizan. Por ejemplo en Guardia Civil tienen su propio PSAP con un CAD para recepción de llamadas al teléfono corto 062, y un SGP compuesto por varios subsistemas: SIGO, SINVES, SIA, ACCEDA, GEISER, …. Aunque posiblemente ya estén conectados sus PSAP con los 112 a través de ESAP-EDXL, hasta hace poco se podía ver agentes de estas policías sentados en las salas de los 112, replicando manualmente los incidentes entre el CAD del 112 y el de su agencia.
Estas agencias tienen unidades especializadas contra el ciberdelito, y para proteger infraestructuras críticas contra ciberataques, integradas se supone, con los sistemas comunes de gestión policial. En España la protección de los sistemas TIC de las propias policías está distribuido en varios niveles, si bien en la Secretaría de Estado de Seguridad que atiende a GC y CNP, se disponen de sistemas de protección perimetral muy avanzados. Si estos sistemas alertan o no a sus unidades contra el delito informático, los autores de este documento lo desconocen aunque parece obvio considerar que sí.

6.1.2 Policías Locales:

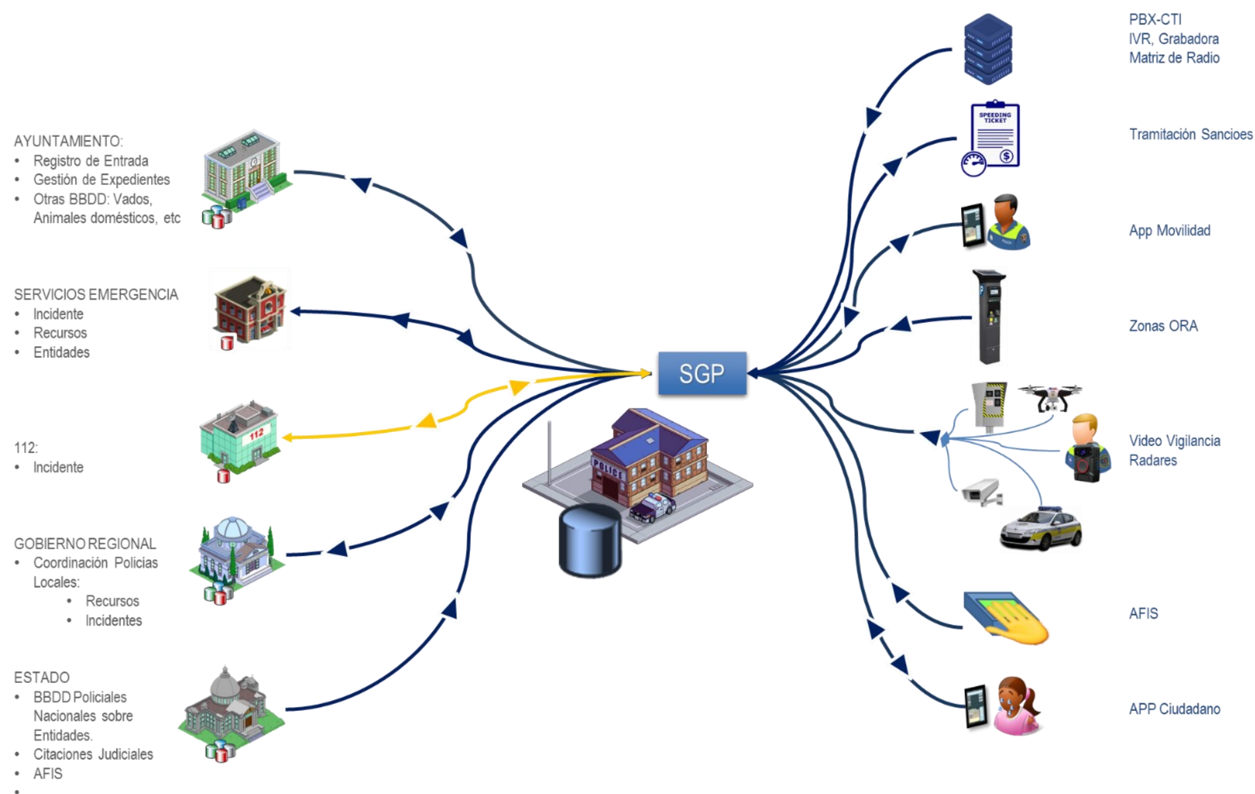
Aunque sorprenda, a fecha de escribir este documento, aun quedan no solo pequeños municipios, sino grandes ciudades que carecen de un sistema específico para la gestión de la Policía Local. Resulta llamativo porque los pequeños municipios con escasos agentes aumentan su nivel de eficacia y disponibilidad, y las policías de grandes ciudades evitan tener personal de "oficina". La "Transformación Digital" es muy beneficiosa para cualquier organización, sobre todo si permite acelerar sus procesos burocráticos, eliminando o reduciendo la intervención humana.

Un municipio "tecnológico", dispone para su Policía Local:

- Sistema de Gestión Policial, con puestos de trabajo en la comisaría.
- Sistema de movilidad del SGP
- Sistema de imposición y tramitación de denuncias de tráfico
- Sistema de Padrón

- Sistema de Administración Electrónica municipal, para el Registro de Entrada y gestión de expedientes.

Complementariamente el 112 puede ofrecerles un terminal para recibir e informar sobre los incidentes asignados. Y en algunos casos disponen de conector vía ESAP-EDXL con el 112.



6.1.3 Protección Civil

En general a nivel municipal no disponen de ningún tipo de sistema TIC. Algunas disponen de terminales de radio, y otras afortunadas usan componentes que los SGP aportan específicamente para las agrupaciones, o si disponen de presupuesto sí tienen sistemas específicos. La función de estos sistemas es la gestión de los incidentes, de la disponibilidad de los voluntarios, y del material, una funcionalidad “reducida” de los SGP como podría entenderse.

6.1.4 Bomberos

La situación de los bomberos es siempre dramática en cuanto a medios materiales y personas. Pocos cuerpos de bomberos disponen de un sistema de gestión de incidentes, parecido al de Policía Local.

Grandes cuerpos de bomberos disponen de soluciones muy potentes para la gestión de la coordinación de los incidentes, integrados telemáticamente con el 112. Además para los bomberos es fundamental la simulación de desastres de cualquier tipo, y representar en el CAD sus efectos.
Los bomberos suelen reclamar el uso de simuladores de desastres naturales como el de TecnoSylva, porque predice lo que puede suceder en un incendio, inundación, nube tóxica, etc. Estos simuladores generan capas “Shape” con los resultados de su simulación. Entonces se pueden importar a un CAD para visualizar la probable evolución del desastre comparado con los datos del suceso real, y poder decidir como actuar.

6.1.5 Agentes Forestales

Realizan una función de policía, custodia y vigilancia del Patrimonio Histórico-Artístico y Arqueológico, y la fauna y flora ubicados en el medio ambiente de la región a la que pertenecen. De todas las agencias es quizás la que menos medios tecnológicos propios tienen por su reciente creación. También determinados departamentos de policías estatales realizan esta función.
Disponen de terminales del CAD del 112 para recibir incidentes y coordinarlos. Sistemas similares a los de una Policía Local podrían ser de directa aplicación.

6.1.6 SEM

Los Servicios de Emergencia Médicos disponen de CAD potentes porque deben ofrecer soporte a protocolos de recepción de llamada, despacho de recursos, y atención médica extrahospitalaria como los de IAED, más complejos que los empleados por policía o bomberos.
Además la variedad de vehículos de rescate y la configuración de los mismos conforme al material y especialidades de sus tripulantes, obliga a ofrecer un soporte “inteligente” al despacho de los recursos.
La integración con los sistemas HIS (Hospital Information Systems) o con los sistemas sanitarios de las regiones, donde está la Histórica Clínica de los ciudadanos, se realiza mediante protocolos internacionales estándares como el HL7 o HAVE-EDXL.

6.1.7 UME

La UME, por su carácter militar inició su andadura con el apoyo de un sistema TIC (CIS por ser militar) de mando y control, adaptado hasta donde fue posible a las emergencias. La UME desarrolló adicionalmente la Red Nacional de Emergencias, un sistema de intercambio de información relevante para la coordinación de las emergencias. La información que comparte es la siguiente:

- Servicios intercambio de ALERTAS y EVENTOS.
- Acceso a una visión compartida de la operación (CROP).
- Servicios METEO y GIS.

- Herramientas colaborativas.
- Servicios de mensajería oficial de emergencias (MOEMER).
- Servicios de telefonía y videoconferencia de emergencias.
- Acceso a otras redes de alerta ajenas a las propias.

El lenguaje CESAR usado por RENEM está basado en TSO Tactic Situation Objects, un estándar XML con fuerte sabor militar, para describir emergencias en un determinado escenario.



Como se observa en este esquema, excepto los centros 112, el resto de agencias no son tenidas en cuenta, si bien no sería necesario si los centros 112 conocieran qué sucede en las agencias que actúan en su jurisdicción administrativa y geográfica.

6.1.8 CiberSOC

Esta agencia consistiría en un centro de monitoreo de las redes públicas para evitar ciberataques contra los ciudadanos, empresas y organismos públicos. Sin embargo hoy en día están desplegados a nivel de las propias organizaciones, no como una "Ciber Policía". El software principal que emplean es de tipo SIEM. Estos sistemas detectan donde se produce una incidencia informática, el tipo de la misma, y coordinan la respuesta para repararla. Como son sistemas procedentes del ámbito empresarial, empleados por el departamento de informática o ciberseguridad, no están diseñados para que reporten a otro sistema de información como un CAD o PSIM.

6.1.9 Esquema Nacional de Interoperabilidad

En España se constituyo el ENI como "un conjunto de criterios y recomendaciones que regulan la manera en la que las Administraciones Públicas de España deben comportarse a la hora de tratar la

información para asegurar la interoperabilidad con sistemas de otras administraciones y con los ciudadanos que hagan uso de la Administración electrónica. Su existencia está contemplada en el artículo 156 de la Ley 40/2015 de Régimen Jurídico del Sector Público”.

Debido a que los servicios de emergencia (Centros “112”, Policía, Bomberos y SEM) son entidades públicas, el ENI debería ser el marco de referencia para las integraciones, para permitir la interoperabilidad entre sistemas TIC usados en las Administraciones Públicas.

Dentro del ENI se define el eXtensible Markup Language (XML) como un estándar válido. Por lo tanto este documento se acotará a soluciones basadas en XML.

En los Centros de Coordinación de Emergencias o 112, EDXL, el lenguaje XML de intercambio de datos sobre Emergencias propuesto por OASIS, está siendo requerido para sus sistemas TIC de manera expresa desde la primera década del siglo XXI, cuando se incluyó como requisito para modelar la información sobre emergencias, en las licitaciones para renovar aplicativos en los centros 112.

Si bien en el ENI se hace referencia al estándar específico de la Factura Electrónica, no hace mención concreta a EDXL. Esperemos que en futuras revisiones del ENI se incluya, puesto que de esta forma los fabricantes e integradores de sistemas TIC en este sector se verían obligados a contemplar este requisito. Y por este motivo, el presente documento ha sido elaborado.

6.1.10 Red de Alerta Nacional de Protección Civil

Uno de los objetivos de la ley española 17/2015, de 9 de julio, del Sistema Nacional de Protección Civil.es “la creación de la Red de Alerta Nacional de Protección Civil como instrumento de comunicación inmediata y de prevención de toda emergencia, al incorporar a los órganos competentes de coordinación de emergencias de las Comunidades Autónomas como cauce para la transmisión de las alarmas a quien corresponda.”

Este objetivo ha sido formulado mediante dos redes:

- RAN: Se crea la Red de Alerta Nacional de Protección Civil como sistema de comunicación de avisos de emergencia a las autoridades competentes en materia de protección civil, sin perjuicio de las competencias de las comunidades autónomas, a fin de que los servicios públicos esenciales y los ciudadanos estén informados ante cualquier amenaza de emergencia.
- RENAIN e crea la Red Nacional de Información sobre Protección Civil con el fin de contribuir a la anticipación de los riesgos y de facilitar una respuesta eficaz ante cualquier situación que lo precise, sin perjuicio de las competencias de las comunidades autónomas. Esta Red permitirá al Sistema Nacional de Protección Civil:

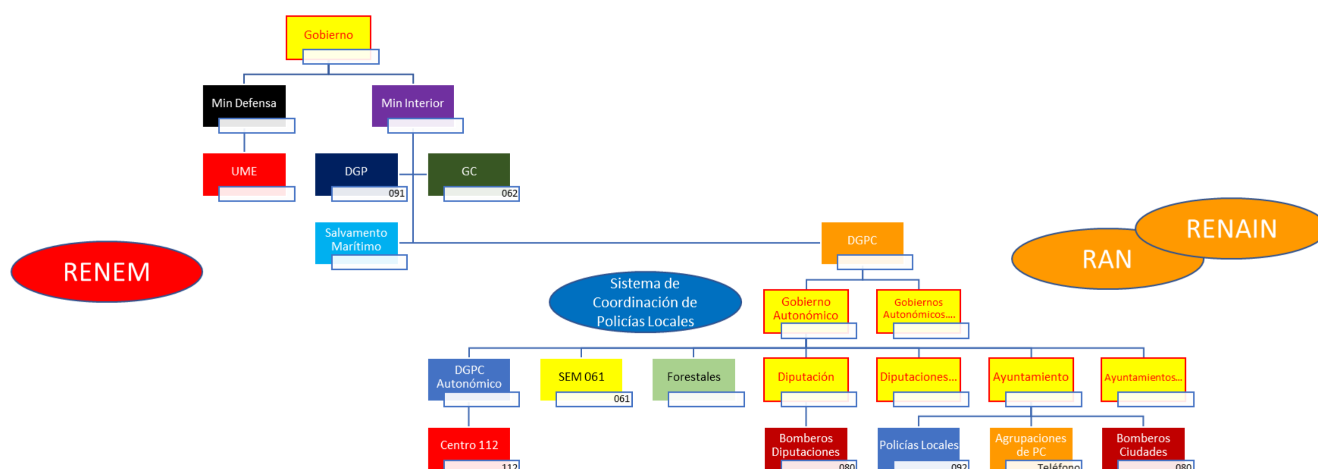
- La recogida, el almacenamiento y el acceso ágil a información sobre los riesgos de emergencia conocidos, así como sobre las medidas de protección y los recursos disponibles para ello.
- Asegurar el intercambio de información en todas las actuaciones de este título.

En ambos casos, estas redes se definirán en el plan nacional de interconexión de información en emergencias, que elaborará el CNSCE previo acuerdo del Consejo Nacional de Protección Civil.

Esperemos que estas redes se definan empleando un lenguaje para compartir información basado en estándares abiertos, porque la industria del sector es pequeña y los proyectos cada vez dotados de menos presupuestos. Adoptar estrategias de interoperabilidad distintas, o definir protocolos propietarios no beneficiará a nadie, ni siquiera a la empresa “estrella” elegida para implementarlo.

Esta ley tiene también como objetivo “fortalecer los centros de coordinación operativa, análogamente a lo que se ha previsto en el Mecanismo de Protección Civil de la Unión Europea con su Centro de Coordinación de Respuesta a Emergencias. Por una parte, se consolidan los órganos competentes de coordinación de emergencias de las Comunidades Autónomas como integrantes esenciales del sistema de protección civil; por otra, se potencia el centro de coordinación actual de la Dirección General de Protección Civil y Emergencias, que se transforma en el Centro Nacional de Seguimiento y Coordinación de Emergencias de Protección Civil, al que corresponde la gestión de las redes de información y alerta del sistema, la interconexión y colaboración con otros centros de coordinación internacionales y constituirse en centro de coordinación operativa desde el cual se dirigirán las emergencias de interés nacional. En estos casos, los órganos competentes de coordinación de emergencias de las Comunidades Autónomas se integrarán operativamente en él, reforzando sinérgicamente la capacidad del sistema.”

La foto conjunta resultante es compleja, y seguro que estamos dejando fuera más de un sistema:



Es obvio que la complejidad es resultante del sistema político que delega responsabilidades de Seguridad a cuatro niveles considerando las Diputaciones.

6.2 Interoperabilidad actual entre las agencias

A continuación se realiza un resumen de como se implementa o no la interoperabilidad entre las distintas agencias. No es una foto pormenorizada ni trata de ser siquiera precisa, puesto que el objeto de este documento no es ese, sino tan solo denotar que en muchos casos la interoperabilidad brilla por su ausencia.

6.2.1 112

Entre los centros 112 y el resto de agencias de despacho, la compartición de datos sobre un incidente, la orden de intervención sucede de las siguientes formas:

- Telefónica: el operador de despacho del 112 llama a la agencia, al número fijo o móvil que tengan establecido, y le comunican el incidente. Entonces finaliza la comunicación y el recurso despachado reporta a su propia agencia. El operador de sala de la agencia puede o no llamar al 112 y decirle como se ha cerrado el incidente.
- Acceso a la aplicación del 112: Algunas agencias tienen en su sala de coordinación un ordenador con acceso a la aplicación del 112. Tienen que atender a la pantalla para conocer los incidentes que se les ha asignado. En esta aplicación reportan datos sobre el estado de actuación, y su cierre.
- Integración telemática entre el 112 y el sistema informático de la agencia. Emplea el formato ESAP- EDXL para un dialogo sostenido y en tiempo real, donde automáticamente el 112 conoce

lo que está haciendo la agencia, sin necesidad de labores de reporte posteriores por parte de la agencia.

6.2.2 Policías

Entre cuerpos policiales ni con otras agencias de despacho, no hay ningún sistema de coordinación automatizado. Todo sucede por medios de comunicación ordinarios: Teléfono, email, e incluso fax. Solo en algunas regiones como Castilla y León y Aragón, o algunas grandes ciudades, las Policías Locales disponen de conexión telemática con los 112.
Las policías autonómicas y estatales no están integradas entre ellas como sería lógico presuponer, al menos con un modelo parecido al de EE.UU.
Es llamativo que las policías estatales tengan todavía su propio número corto, "091" y "062", y que no reporten automáticamente a los 112 de estos incidentes cuando requieren de la intervención de otras agencias. En pocos casos hay una integración telemática entre los sistemas 112 y los de las policías (Nacionales, Regionales o Locales de grandes ciudades). Todavía hay en las salas 112 operadores de estas agencias que replican los avisos de la aplicación 112 a la suya propia.

El formato de intercambio de información con los juzgados, otros organismos o con los ciudadanos es a través de sistemas de administración electrónica, que suelen concretarse en documentos PDF o incluso en papel impreso como por ejemplo las multas.

6.2.3 Bomberos

Por su relación con el 112, al disponer de operadores de despacho en los PSAP, es el único punto de contacto digital con otras agencias. Entre cuerpos de bomberos, o con otras agencias de despacho, no hay ningún sistema de coordinación automatizado. Todo sucede por medios de comunicación ordinarios: Teléfono, email, e incluso fax.

6.2.4 Protección Civil

La relación con los 112 es gracias a las llamadas directas entre ambos organismos, o por disponer de un terminal del 112, como sucede con Policía Local.
Todos los intercambios de información suceden por medios de comunicación ordinarios: Teléfono, email, e incluso fax. Hay software de Policía Local que incorpora funcionalidades para P. Civil, pero no tiene habilitada la capacidad de despachar incidentes de manera telemática entre ambas agencias municipales, pero aun así se atreven a denominarse "multiagencia", cuando tan solo son capaces de transferir el incidente a otras agencias.

6.2.5 Forestales

Similar al caso de los Bomberos o P. Civil.

6.2.6 SEM

Los servicios públicos de ambulancias en España, por ser de ámbito regional, sí están plenamente integrados con los centros 112, pese a que muchos mantienen su propio número corto "061".
No lo están las organizaciones como Cruz Roja, ni tampoco las ambulancias de empresas de salud privadas.

6.2.7 UME

La UME ofrece accesos a RENEM a cualquier agencia o centro 112. Se desconoce por los autores del documento si tan solo la UME recopila datos de las agencias de despacho, o si ofrece algo más. En futuras revisiones de este documento se aportará más información si es abierta, y si corrige esta apreciación.

6.2.8 CiberSOC de titularidad estatal, autonómica o local

Son servicios de muy reciente creación, y realmente todavía pocos los consideramos como parte del sistema de gestión de emergencias.
Los ciberSOC están dotados de potentes herramientas de monitoreo, y de software preventivo, reactivo y para realizar ciberataques, como por ejemplo los de tipo SIEM. Sin embargo no prestan atención a la necesaria comunicación de los eventos detectados con el responsable de seguridad de la organización: No hay implementado un sistema que correlacione los sistemas afectados por un ciberataque con los activos físicos que pueden resultar dañados.

7 Requisitos de Interoperabilidad

En este capítulo se recopilan los requisitos de interoperabilidad de cada agencia con las otras, que permitirían una colaboración por encima de trabas políticas o burocráticas.

7.1 Elementos de interoperabilidad

A continuación se enumeran de forma no exhaustiva ni de manera general para todas las agencias, los datos que tienen **necesidad de conocer** en determinadas circunstancias. Estos datos están mejor detallados en los lenguajes EDXL específicos, pero sirven para visualizar la complejidad y riqueza de los datos necesarios para comprender un suceso.

- Entidades
    - Personas
        - Filiación
        - Historial clínico
        - Antecedentes penales
        - …
    - Domicilios
    - Empresas u organismos
        - Propietario
        - Teléfono
        - Email
        - Empresa de seguridad
            - Teléfono
        - Tipo de negocio
        - Ubicación del Plan de Emergencias y Autoprotección
        - Responsable de PRL
    - Vehículos
    - Animales
    - Teléfonos
    - Correos electrónicos
    - Perfiles en redes sociales
    - Número de cuentas corrientes
    - Número de tarjetas bancarias
    - IMEI de tarjetas SIM
    - MAC de dispositivos informáticos
    - IP de dispositivos informáticos

- …
- Incidentes
    - Identificador único del incidente
    - Fecha y hora del incidente
    - Ubicación
    - Tipo del incidente
    - Descripción del incidente
    - Personas víctimas
    - Personas detenidas
    - Personas testigos
    - Propiedades dañadas
    - Agencias despachadas
    - Comunicaciones entre el despachador y las agencias
    - Material multimedia que documenta el incidente
    - …
- Recursos de la agencia
    - Identificador del recurso
    - Estado del recurso
    - Equipamiento del recurso
    - Ubicación del recurso
    - Velocidad
    - Autonomía remanente
    - Temperatura del habitáculo
    - Estado de actuación del recurso respecto a un incidente
    - Hora finalización de su turno
    - Id de su canal de radio
    - Número de teléfono móvil
    - Nombre de los agentes que lo tripulan y sus especialidades
    - …
- Caso o Expediente
    - ID del Incidente que lo desencadena
    - ID único del Expediente
    - Autor del expediente
    - Documentos del expediente
        - Evidencias
        - Declaraciones
        - …
    - …

Estos tipos de datos pueden ampliarse para recoger nuevos tipos de elementos, pero debería hacerse siguiendo un esquema común, un mismo lenguaje para simplificar la comunicación entre sistemas que coexisten en este mismo entorno.

7.2 Intercambio de información entre agencias

A continuación se enumera de forma no exhaustiva la información que las diferentes agencias deberían compartir con las restantes para disponer todos de una foto exacta de lo que sucede, acotada por sus competencias y jurisdicciones administrativas y geográficas.

Esta tabla refleja el modelo español, donde los centros 112 son o deberían ser los que coordinan todas las emergencias. La UME coordina la respuesta a incidentes que afectan a más de una región. Otras coordinaciones entre agencias puede que no sean precisas o incluso reales, pero se trata simplemente de denotar qué informaciones tendría lógica que intercambiaran.

Envían / Reciben.	Centros 112	Policías Estatales	Policías Regionales	SEM	Bomberos	Policías Locales	P. Civil	UME	CiberSOC
Centros 112	Incidentes Entidades	Incidentes	Incidentes	Incidentes	Incidentes	Incidentes	Incidentes	Incidentes	Incidentes
Policías Estatales	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos
Policías Regionales	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos
SEM	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos
Bomberos	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos

Policía Local	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos
P. Civil	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos
UME	Incidentes Recursos	Incidentes Recursos	Incidentes Recursos	Incidentes Recursos	Incidentes Recursos	Incidentes Recursos	Incidentes Recursos		Incidentes Recursos
CiberSOC	Incidentes Recursos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Recursos Casos	Entidades Incidentes Recursos Casos	Entidades Recursos Casos

Llevado al extremo, la comunicación entre una agencia de despacho y otra debería consistir en un sistema CAD2CAD, que permitiera gestionar y consultar:

- Estado en tiempo real de los recursos propios
- Petición de recursos de la otra agencia
- Consultar el estado operacional de la otra agencia, pudiendo modificar los despachos de sus propios recursos.
- Consultas sobre informes, protocolos, uso de recursos,

Un proyecto de implementación de un sistema CAD2CAD entre las agencias de una región requiere de un bus de integración como plataforma base, tipo BizTalk, Tibco, … y muchas jornadas de trabajo. Por lo que una solución COTS sería lo más recomendable. En España o LATAM no existe este tipo de soluciones porque los usuarios no lo demandan por cuestiones políticas ajenas al alcance de este documento, lo que no significa que no sean conscientes de los beneficios que aportaría poder ejercer su necesidad de conocer.

7.3 Fuentes y tipos de datos

La siguiente tabla contiene también de forma no exhaustiva, los requisitos de acceso a fuentes de información de cada agencia:

Fuente / Sistema	Llamadas al 112	Llamadas directas	Agentes	Agencias colaboradoras	Video Vigilancia	Gestión de Flota	Sensores	Fuentes RSS	Medios de Comunicación	RRSS	Intranet, Web, DeepWeb, DarkNet
Centros 112	Sí	Sí	No tiene agentes propios.	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Policías Estatales	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí
Policías Regionales	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
SEM	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Bomberos	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
Policía Local	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
P. Civil	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
UME	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	Sí	No
CiberSOC	Sí	Sí	Sí	Sí	Sí	No	Sí	Sí	Sí	Sí	Sí

Sin considerar los aspectos legales sobre el acceso a estas fuentes de información, lo destacable es que hoy en día las fuentes de datos a las que se necesitan accesos son:

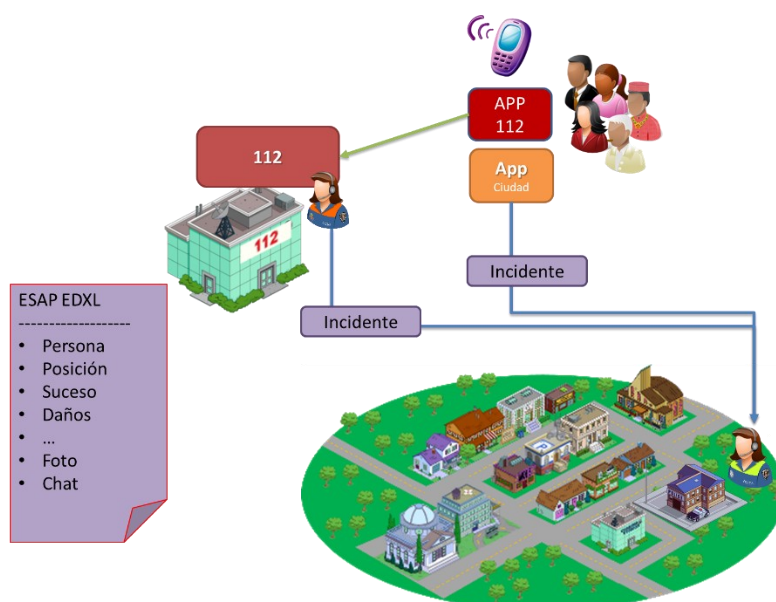
- Video Vigilancia
- Gestión de Flota
- Sensores (IoT, SOC, …)
- Fuentes RSS
- Medios de Comunicación
- RRSS
- Aquella que ayude a comprender la escena.

Solo las policías integrales y el CiberSOC tienen interés especial hoy en día en conocer lo que sucede en la Intranet de la organización, la Web, DeepWeb y DarkNet, pero si lo que sucede en ese dominio afecta a otro dominio, entonces deben ser capaces de alertar a otras agencias.

Sin embargo las Policías Locales deberían gestionar de alguna la ciberseguridad de al menos las infraestructuras TIC municipales, igual que gestionan las CRA de los edificios y sus controles de acceso. El cibercrimen, no es más que el crimen tradicional pero en el ciberespacio.

7.3.1 Ejemplo: App de ciudadanos

En el siguiente gráfico se representa un modelo de cómo debería ser conforme a criterios de racionalidad, que no se solapen funcionalidades entre los diferentes sistemas, la comunicación entre las aplicaciones de movilidad para que los ciudadanos puedan reclamar la asistencia de los servicios de emergencia. La llamada sigue siendo el medio convencional, si bien las “app 112”, que empleando el protocolo PEMEA definido por EENA.org, pueden dialogar con los 112. En los municipios hay dos frentes: empresas que ofrecen servicios de valor añadido a los ciudadanos mientras proporcionan otros específicos a los ayuntamientos, y las app creadas por el municipio.



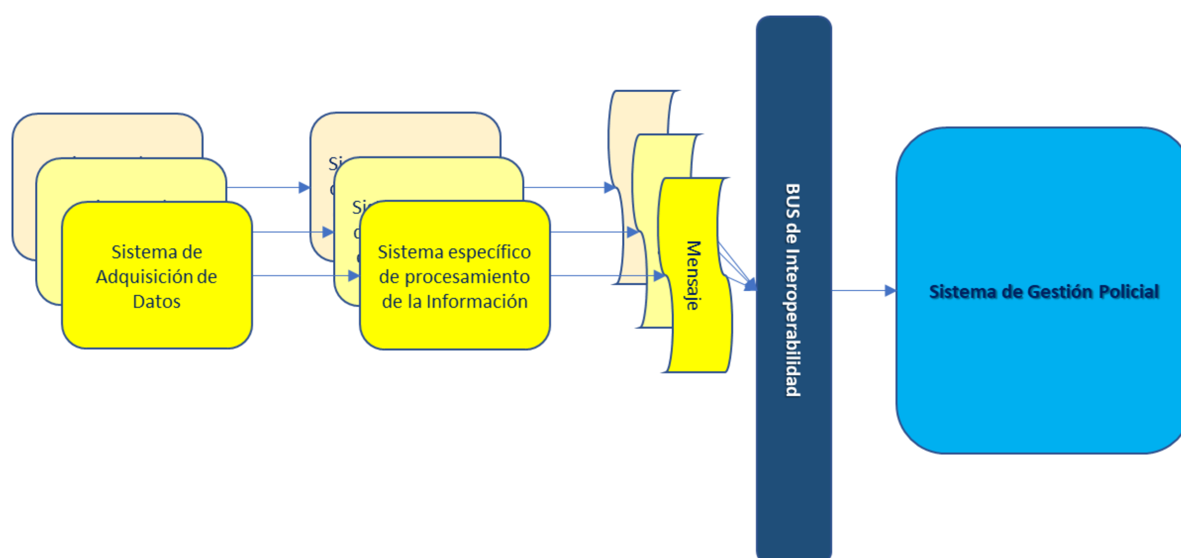
En este gráfico se propone como protocolo de comunicación entre las diferentes APP municipales, el uso del mismo protocolo que existe para que el 112 hable con los servicios de emergencia municipales. El beneficio es "liberalizar" el acceso digital a las agencias municipales, igual que un francés con su app 112 nacional, puede interactuar con el 112 de cualquier región española cuando se encuentra en ella. Además, las app 112 podrían añadir la capacidad de hablar directamente con los municipios, que como ventaja tiene la reducción de tiempos al responder: La Policía Local es generalmente la primera en responder. Debemos recordar que no todos los ciudadanos disponen de móviles de alta gama capaces de soportar decenas de aplicaciones diversas, ni tienen ánimo para instalar, configurar ni aprender a usar nuevas aplicaciones.

8 Lenguajes de Interoperabilidad

Como se ha podido seguir en este documento, existen lenguajes de interoperabilidad suficientes en el mercado para poder estandarizar el idioma que hablen las diferentes aplicaciones de las agencias.
El siguiente cuadro resume los diferentes estándares, aunque quizás algunos deberían añadir modificaciones para ajustarse a requisitos específicos, que podrían emplearse para establecer un diálogo entre estos diferentes sistemas:

Software de Agencia / Sistema	CAD 112	CAD de Agencia	RMS	SVP	Gestión de Flota	Sensores	Fuentes RSS	Hospitales	PSIM	CiberSOC
CAD 112	ESAP DE SITREP	ESAP DE HAVE RS SITREP TEP	No Aplica	CAP RTSP	RS	CAP	CAP	HAVE TEP HL7	CAP	CAP
CAD	ESAP DE SITREP	RS DE CAP CAD2CAD	DE RS TEP	CAP RTSP	RS	CAP	CAP	HAVE TEP HL7	CAP	CAP
C4RSI (UME)	CESAR	CESAR	No Aplica	CAP RTSP	RS	CAP	CAP	HAVE TEP HL7	No Aplica	CAP
RMS	No Aplica	DE RS	No Aplica	CAP	RS	CAP	CAP	No Aplica	No Aplica	No Aplica
CyberSOC	CAP	CAP	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	CAP
Apps 112	PEMEA CAP	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica

Apps Municipales	No Aplica	ESAP CAP	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica
Botón de Pánico	CAP	CAP	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica



8.1 Comunicación con sistemas corporativos

Aunque no es objeto de este documento la integración de los Sistemas de Gestión de Emergencias (SGE) con los sistemas de gestión administrativa o ERP de los organismos a los que pertenezcan, o con los que deban colaborar, estos suelen tener que consultar o dialogar con esos otros sistemas para comunicar la actividad realizada por los recursos humanos y materiales, etc. Por ejemplo citamos los siguientes:

- BBDD ANI/ALI (Operadoras de Telecomunicaciones o Agencias Estatales que regulan el sector)
- Registro Civil (Estatal)
- Padrón Municipal (Municipal)
- Registro de Entrada
- Sistema de RRHH
- Registro de Vehículos
- Registro de Animales Domésticos

- Registro de personas con antecedentes criminales
- Registro de Tributos para el pago de tasas y sanciones
- Registro de bienes inmuebles o Catastro
- Sistema sanitario

Como en el caso de sistema sanitario, donde se emplean los protocolos HL7 o HAVE-EDXL, es necesario definir estándares de interoperabilidad con estos sistemas. Por ejemplo para ANI/ALI existe un estándar propuesto por NENA.org.

Habitualmente las integraciones entre un CAD y los sistemas municipales se resuelven con métodos que suponen lastres en el evolutivo y mantenimiento a largo plazo de la solución:

- Accesos directos a las bases de datos de terceras aplicaciones, que obligará a volver a desarrollar el "conector" cuando alguno de los dos sistemas sufra cualquier modificación o se reemplaza alguno de ellos
- Uso de API de alguno de los dos sistemas que deben dialogar, que si bien debería aislar el "conector" de cambios de versiones entre ambos sistemas, tan solo significa un ligero decremento en el coste de construcción y mantenimiento del conector.

En el caso de conectividad entre la base de datos de ciudadanos y el CAD de la Policía Local, vital para acelerar el proceso de identificación del llamante, si el Sistema de Gestión del Padrón y el CAD usaran ambos el protocolo ANI/ALI propuesto por NENA, no haría falta que el cliente final tuviera que preocuparse sobre esta integración.

Sin embargo, los fabricantes de software de Padrón habituales en España, por ser su cliente principal las aplicaciones de Administración Electrónica, en muchos casos parte de la misma "Suite" de productos de un mismo fabricante, como mucho ofrecen un API o webservices para consultar esta base de datos, sin comprometerse a no variar estos componentes en nuevas versiones.
A esto se añade que como el mercado de la Administración Pública Municipal es pequeño, los fabricantes de soluciones para municipios no ofrecen por lo general a sus "partners tecnológicos" entornos de pruebas de integración, lo que obliga al cliente final a tener que soportar en el entorno de producción fallos y caídas de los sistemas de Producción mientras se realizan los trabajos de integración.

Por lo tanto, se recomienda a los clientes finales que exijan a los fabricantes de soluciones, no ya que ofrezcan un API, sino que empleen estándares abiertos de interoperabilidad para hablar con otros sistemas. O al menos ofrezcan la documentación técnica del protocolo propietario usado. En el peor de los casos, bastaría con hacer una traducción del protocolo propietario a uno estándar para aislar los problemas anteriormente enunciados:

- **Elevados costes y plazos** para las integraciones

- **Costes de mantenimiento** de los conectores ante cambio de versiones

Pero hay otro elemento más a ser tenido en cuenta: **Punto único de fallo o SPOF**. Los sistemas de gestión de emergencias no pueden depender de terceras partes. Si el Padrón no responde con los datos, el Sistema de Gestión Policial no puede quedarse "colgado", "congelado" o "frito", debe poder seguir trabajando. Es decir, la comunicación entre los sistemas debe ser asíncrona. Y llevado al extremo, **multicanal** para evitar que por la caída de un medio de comunicación los sistemas dejen de dialogar (TIER4)

8.2 Beneficio para todos

La estandarización en la comunicación entre sistemas informáticos, produce beneficios para todos. Para los clientes, entre otros:

- Evitar **costes asociados a las integraciones**.
- **Coste nulo del mantenimiento** de los conectores si el protocolo mantiene la compatibilidad con versiones anteriores del mismo.
- Puestas en producción que **no dependen** de las integraciones.
- **Plazos cortos** para los proyectos de implantación
- Asegurar la **mantenibilidad, escalabilidad y mejoras evolutivas** del sistema global, al **no depender** de ninguna pieza del mapa de soluciones.

Y para la Industria, entre otros:

- Evitar daños a su reputación, o cancelaciones de contratos, por las pruebas de integración realizadas en el entorno de Producción del Cliente.
- Evitar conflictos con los responsables de terceras soluciones por no colaborar adecuadamente en las integraciones.
- Eliminación en los procesos de compra, los requisitos de integración imposibles de cumplir o de demostrar, como por ejemplo "deberá disponer de conector con la aplicación Fulana, y justificarla mediante al menos 3 proyectos realizados en los últimos 3 años".

9 Como integrar

En este capítulo se tratará someramente las formas de integración posibles usando estándares y buenas prácticas que permitan la escalabilidad, mantenibilidad del sistema resultante.

9.1 112 con agencias de despacho

El lenguaje ya propuesto, aceptado e implantado es el ESAP-EDXL. Este lenguaje permite enviar a una agencia de despacho un incidente, con todos los datos que sean precisos incluyendo datos multimedia, a las agencias que deban intervenir, y facilitar que estas agencias desde su software de gestión reporten al 112 sobre su actuación.

El mensaje ESAP contiene la información de datos de emergencias que son necesarios para la gestión de la emergencia. El protocolo ESAP está encapsulado dentro de la familia de protocolos EDXL de OASIS. Ha sido creada por Telefónica para mejorar el intercambio de información entre centros coordinadores de emergencias y organismos que disponen de recursos para resolverlas.

Luego para que opere esta conexión, tanto el sistema CAD del PSAP como el de la agencia, deben implementase en cada lado unos servicios web que permitan el diálogo con ESAP-EDXL entre ambas agencias.

En algunos casos para simplificar la construcción de servicios web, uno por cada agencia, se puede optar por un **EAI**, que simplifique en el lado del 112 esta conectividad, y sea el agregador el que se encargue de hablar con las agencias de despacho de la región.

Esta arquitectura permite hablar desde el 112 con cualquier agencia, independientemente del software que utiliza cada una de ellas.

No aplica el modelo CAD2CAD porque el PSAP no asigna incidentes a recursos físicos.

9.2 PSAP 112 con Apps 112 de ciudadano

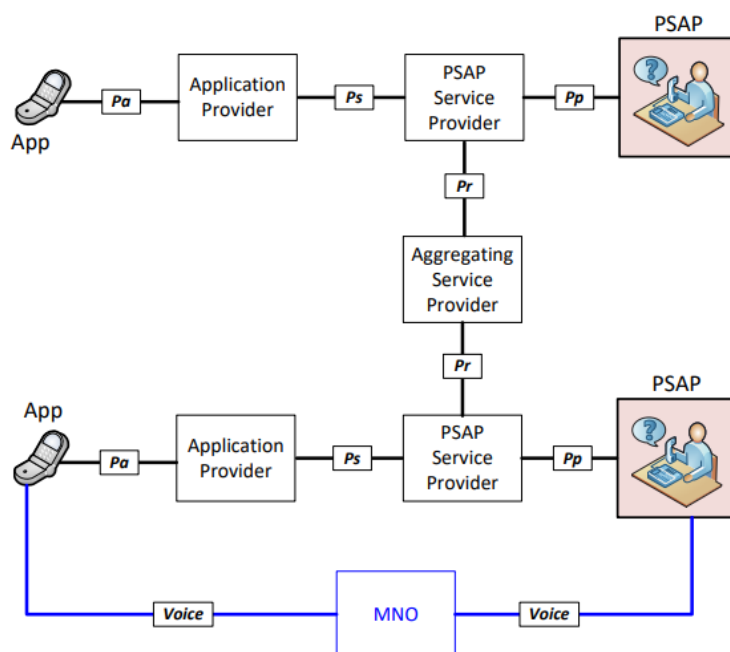
No se ha incluido anteriormente este tipo de sistemas informáticos, porque no están necesariamente relacionados con los PSAP, pero se comunican con ellos.

El estándar aplicable es PEMEA, definido por EENA.org.

Arquitectura:

- App, es la parte cliente- su función es de llamar al 112

- Proveedor de Aplicación (AP) autentica a los usuarios, formatea los datos de la llamada antes de enviar la información al Proveedor de Servicio (PSP)
- PSP coge los datos de la persona que llama a partir de fuentes de confianza y proporcionar al PSAP
- Si el usuario está en itinerancia, los datos se envían al ASP para fines de enrutamiento.
- ASP proporciona enrutamiento de datos para el correcto PSP / PSAP, o envía un error.
- PSAP obtiene la información que necesita, la persona que llama recibe la ayuda necesaria.



Los datos intercambiados entre la app del ciudadano y el PSAP son:

- Llamada de voz
- Datos sobre ubicación, médicos, …
- Chat
- Video conferencia,

9.3 Apps vecinales con las Agencias

Existen aplicaciones como Línea Verde o M7, permiten que el ciudadano se comunique con el Ayuntamiento para muy variadas funciones, pero también para cuestiones de seguridad.
Para simplificar el proceso de esta información, el esquema lógico es que la aplicación municipal envíe el incidente "policial" al SGP, para evitar que el agente tenga que usar otra aplicación adicional para cuestiones del mismo tipo.

EL proceso lógico de integración puede ser alguno de los tres siguientes, ya que la App actúa a modo de App 112:

A. Comunicación bidireccional:
    1. Entre el SGP y la App vecinal debería hablarse con el protocolo PMEA, ya que la Policía Local actúa como PSAP.
    2. El protocolo sería ESAP-EDXL si existe una figura intermedia que verifica la autenticidad de los mensajes y los clasifica.

B. Comunicación Unidireccional:
    3. Si la App no espera recibir notificación de la agencia, el protocolo CAP sería más que suficiente. Por ejemplo una app de botón de pánico aunque la aplicación active una llamada de voz al 092.

Lo que no tiene sentido son soluciones existentes tipo “App Ciudadano” que solapan no solo la recepción de avisos sino también de manera parcial el despacho y procesos administrativos asociados. Quizás el objetivo de los fabricantes de estas soluciones es crecer hacia un CAD, pero mientras lo logran, obligan al servicio de emergencias a trabajar por duplicado, o a tener la información en múltiples silos independientes.

9.4 CAD con CAD

Para que una agencia, por ejemplo una policía local pueda colaborar con otra policía aportando o requiriendo recursos, se deberían emplear todo tipo de paquetes EDXL.
Existen aplicativos COTS “CAD2CAD” que proporcionan las herramientas necesarias para configurar y monitorizar las transacciones entre ambos sistemas.

9.5 CAD con RMS

En España este tipo de integración solo tiene sentido para las grandes policías estatales, regionales o municipales. Normalmente se implementa una conexión unidireccional básica, consistente en pasar el incidente al sistema de gestión de los trabajos de policía administrativa y judicial.

Sin embargo hay regiones que desean que sus Policías Locales se coordinen de manera estrecha y una plataforma de interoperabilidad entre todas las agencias, sin llegar a ser un CAD2CAD seria fácilmente implementable si los CAD de cada agencia, independientemente de su fabricante, hablaran protocolos EDXL.

9.6 CAD con SVP

En este apartado se va a detallar más en profundidad como integrar estos sistemas debido a la urgencia que existe en la actualidad. Se implantan muchos Sistemas de Video Vigilancia sin integración con el SGP, y los fabricantes de SGP están muy desorientados al respecto puesto que pretenden añadir funciones VMS dentro de sus productos, o no captan la potencia de esta fuente de inteligencia.

9.6.1 Visualizar desde el CAD las cámaras

Para poder visionar la imagen de una cámara desde un tercer sistema, en este caso un CAD, existen protocolos estándar, como por ejemplo el RTSP que permiten hacer un visionado en directo de las imágenes captadas por las cámaras.

La implementación sobre el mapa, sobre el interfaz GIS permite no solo ver la cámara más cercana al incidente, sino capturar imágenes o secuencias para ser retransmitidas a los recursos despachados, o para adjuntarlos al incidente. Saber lo que se va a encontrar el respondedor es vital para que este se prepare adecuadamente antes de llegar al lugar de los sucesos.

9.6.2 Recibir eventos desde las cámaras

Se tiene constancia que para integrar los cinemómetros, los fabricantes de estos sistemas y los de SGP intercambian los siguientes datos:

- Id del Radar
- Coordenadas en grados de la ubicación del radar.
- Dirección postal o punto kilométrico
- Dia y hora
- Matrícula leída en algunos casos.
- Fotos del vehículo, tres según la legislación española.
- Velocidad del vehículo o exceso de velocidad.

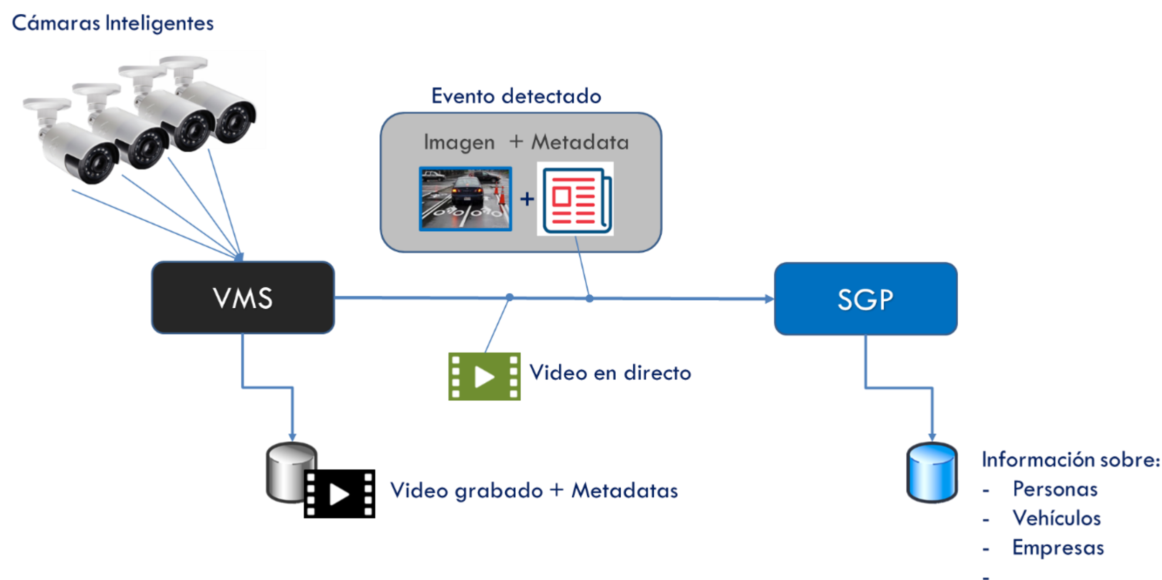
En el SGP se consulta contra las BBDD de vehículos disponibles, y se compone automáticamente el boletín de denuncia con los datos obtenidos, indicando el importe de la sanción según la velocidad que llevara el vehículo.

Esta misma comunicación sucede con los sistemas de tramitación de denuncias que no requieren de un SGP.

El método básico de comunicación consiste en depositar en un sistema de archivo estos datos, o incluso nombrar las fotos realizadas con los datos requeridos.

La forma correcta consiste en empaquetar estos datos en un XML o JSON para universalizar el protocolo de comunicación. Es de destacar que la comunicación es unidireccional, donde el SVP emite

cuando se genera un evento, mientras que el SGP está permanentemente a la escucha de nuevos eventos.



9.6.2.1 Estandarización de los eventos

Para el diálogo entre el SGP y el SVP se considera que la forma adecuada, conforme al estado de arte informático actual, debe ser mediante servicios web, que intercambien mensajes en formato XML o JSON conforme a estándares abiertos específicos en el sector de la Seguridad Pública.

9.6.2.2 Metadata del evento

Como se ha descrito anteriormente para el caso del radar de velocidad, la información es muy simple. Para nuevos eventos, bastaría con añadir el tipo del evento detectado para universalizar el mensaje:

- Id de la cámara o radar
- Coordenadas en grados de la ubicación del radar.
- Dirección postal o punto kilométrico
- Dia y hora
- Tipo de evento detectado: Exceso velocidad | Stop | Semáforo en rojo | aparcamiento indebido | Acceso no autorizado a ZBE | Circulación en sentido contrario | Invasión de zona peatonal | etc.
- Matrícula leída
- Fotos del vehículo durante la infracción.
- Enlace a la grabación
- Valor numérico en caso de exceso de velocidad, exceso de peso, exceso de longitud, …

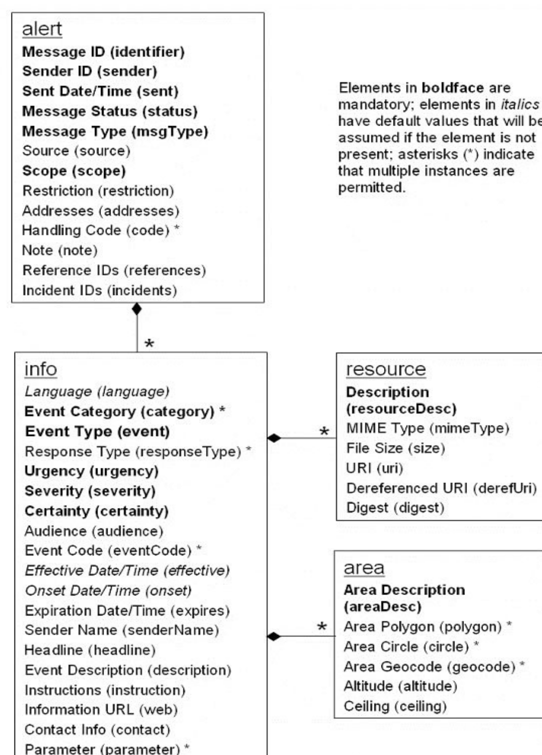
Esta metadata en formato EDXL se puede adecuar fácilmente al CAP.

9.6.3 Common Alert Protocol

El uso principal del mensaje de alerta CAP es proporcionar una entrada única para activar todo tipo de sistemas de alerta y advertencia pública. Esto reduce la carga de trabajo asociada con el uso de múltiples sistemas de alerta al tiempo que mejora la confiabilidad técnica y la efectividad del público objetivo. También ayuda a garantizar la coherencia en la información transmitida a través de múltiples sistemas de entrega, otra clave para la efectividad de las advertencias.
Una aplicación secundaria de CAP es normalizar las advertencias de varias fuentes para que puedan agregarse y compararse en forma tabular o gráfica como ayuda para el conocimiento de la situación y la detección de patrones.
Aunque se diseñó principalmente como un estándar de interoperabilidad para su uso entre sistemas de alerta y otros sistemas de información de emergencia, el mensaje de alerta CAP se puede enviar directamente a los destinatarios de la alerta a través de varias redes, incluidas las transmisiones de datos. Los dispositivos receptores con reconocimiento de ubicación podrían utilizar la información de un mensaje de alerta CAP para determinar, en función de su ubicación actual, si ese mensaje en particular era relevante para sus usuarios.
El mensaje de alerta CAP también puede ser utilizado por los sistemas de sensores como un formato para informar eventos significativos a los sistemas y centros de recolección y análisis.
Las palabras advertencia, alerta y notificación se usan indistintamente a lo largo de este documento.
El término “par de coordenadas” se utiliza en este documento para referirse a un par de valores decimales delimitados por comas que describen una ubicación geoespacial en grados,

Estructura del Mensaje de Alerta CAP: Cada mensaje de alerta CAP consta de un segmento <alert>, que puede contener uno o más segmentos <info>, cada uno de los cuales puede incluir uno o más segmentos <area> y/o <resource>. En la mayoría de las circunstancias, los mensajes CAP con un valor <msgType> de "Alerta" DEBERÍAN incluir al menos un elemento <info>.

- <alert> El segmento <alert> proporciona información básica sobre el mensaje actual: su propósito, su fuente y su estado, así como un identificador único para el mensaje actual y enlaces a cualquier otro mensaje relacionado. Un segmento de <alerta> puede usarse solo para confirmaciones de mensajes, cancelaciones u otras funciones del sistema, pero la mayoría de los segmentos de <alerta> incluirán al menos un segmento de <info>.



- <info> El segmento <info> describe un evento anticipado o real en términos de su urgencia (tiempo disponible para prepararse), severidad (intensidad del impacto) y certeza (confianza en la observación o predicción), además de proporcionar descripciones categóricas y textuales de el evento sujeto. También puede proporcionar instrucciones para una respuesta apropiada por parte de los destinatarios del mensaje y varios otros detalles (duración del peligro, parámetros técnicos, información de contacto, enlaces a fuentes de información adicionales, etc.) Se pueden usar varios segmentos de <info> para describir diferentes parámetros (p. ej., para diferentes “bandas” de probabilidad o intensidad) o para proporcionar la información en varios idiomas.
- <resource> El segmento <resource> proporciona una referencia opcional a información adicional relacionada con el segmento <info> dentro del cual aparece en forma de activo digital, como una/s **imagen o un archivo de audio o vídeo**.
- <area> El segmento <area> describe un área geográfica a la que se aplica el segmento <info> en el que aparece. Se admiten descripciones textuales y codificadas (como códigos postales), pero las representaciones preferidas usan formas geoespaciales (polígonos y círculos) y una altitud o rango de altitud, expresado en términos estándar de latitud/longitud/altitud de acuerdo con un dato geoespacial específico

Más información en http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html

9.6.3.1 Modelado del evento para el SVP en formato CAP-Tráfico

```
<?xml version = "1.0" encoding = "UTF-8"?>
<!-- Copyright OASIS Open 2010 All Rights Reserved -->
<!-- Versión Video Vigilancia Policial por Asociación ITEM. -->
```

```
<schema xmlns = "http://www.w3.org/2001/XMLSchema"
   targetNamespace = "urn:oasis:names:tc:emergency:cap-Tráfico:1.0"
   xmlns:cap = "urn:oasis:names:tc:emergency:cap:1.2"
   xmlns:xs = "http://www.w3.org/2001/XMLSchema"
   elementFormDefault = "qualified"
   attributeFormDefault = "unqualified"
   version = “1.2”>
  <element name = "alert">
    <annotation>
      <documentation>CAP Alert Message (version 1.2)</documentation>
    </annotation>
    <complexType>
      <sequence>
        <element name = "identifier" type = "xs:string"/>
        <element name = "sender" type = "xs:string"/>
        <element name = "sent">
          <simpleType>
            <restriction base = "xs:dateTime">
             <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
           </restriction>
          </simpleType>
        </element>
        <element name = "status">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Actual"/>
              <enumeration value = "Draft"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "msgType">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Alert"/>
              <enumeration value = "Error"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "source" type = "xs:string" minOccurs = "0"/>
        <element name = "scope">
          <simpleType>
            <restriction base = "xs:string">
              <enumeration value = "Private"/>
            </restriction>
          </simpleType>
        </element>
        <element name = "restriction" type = "xs:string" minOccurs = "0"/>
        <element name = "addresses" type = "xs:string" minOccurs = "0"/>
        <element name = "code" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
        <element name = "note" type = "xs:string" minOccurs = "0"/>
        <element name = "references" type = "xs:string" minOccurs = "0"/>
        <element name = "incidents" type = "xs:string" minOccurs = "0"/>
        <element name = "info" minOccurs = "0" maxOccurs = "unbounded">
          <complexType>
            <sequence>
              <element name = "language" type = "xs:language" default = "en-US" minOccurs = "0"/>
              <element name = "category" maxOccurs = "unbounded">
                <simpleType>
                  <restriction base = "xs:string">
                    <enumeration value = "Matrícula"/>                    / Posibles infracciones de tráfico
                    <enumeration value = "Velocidad máxima"/>
                    <enumeration value = "STOP"/>
                    <enumeration value = "Foto Rojo"/>
                    <enumeration value = "Acceso no autorizado a ZBE"/>
                    <enumeration value = "Interés Policial"/>
```

```
        <enumeration value = "Sentido Contrario"/>
        <enumeration value = "Circulación prohibida"/>
        <enumeration value = "Entrada prohibida"/>
        <enumeration value = "Giro prohibido"/>
        <enumeration value = "Adelantamiento prohibido"/>
        <enumeration value = "Parada y estacionamiento prohibido"/>
        <enumeration value = "Estacionamiento prohibido"/>
        <enumeration value = "Advertencias acústicas prohibidas"/>
        <enumeration value = "Adelantamiento prohibido"/>
        <enumeration value = "Uso obligatorio cinturón"/>
        <enumeration value = "Paso de peatones"/>
        <enumeration value = "Circulación negligente"/>
        <enumeration value = "Other"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "event" type = "xs:string"/>
  <element name = "responseType" minOccurs = "0" maxOccurs = "unbounded">
    <simpleType>
      <restriction base = "xs:string">
        <enumeration value = "Alerta"/>                       /Tipo de Alerta
        <enumeration value = "Aviso"/>
        <enumeration value = "Boletín"/>
        <enumeration value = "None"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "urgency">
    <simpleType>
      <restriction base = "xs:string">
        <enumeration value = "Immediate"/>                    /Urgencia de la Alerta
        <enumeration value = "Planned"/>
        <enumeration value = "Scheduled"/>
        <enumeration value = "Unknown"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "severity">
    <simpleType>
      <restriction base = "xs:string">                        /Valoración de la Alerta
        <enumeration value = "Extreme"/>
        <enumeration value = "Severe"/>
        <enumeration value = "Moderate"/>
        <enumeration value = "Minor"/>
        <enumeration value = "Unknown"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "certainty">
    <simpleType>
      <restriction base = "xs:string">
        <enumeration value = "Observed"/>                     /Credibilidad de la Alerta
        <enumeration value = "Possible"/>
        <enumeration value = "Unknown"/>
      </restriction>
    </simpleType>
  </element>
  <element name = "audience" type = "xs:string" minOccurs = "0"/>
  <element name = "eventCode" minOccurs = "0" maxOccurs = "unbounded">
    <complexType>
      <sequence>
        <element ref = "cap:valueName"/>
        <element ref = "cap:value"/>
      </sequence>
    </complexType>
```

```
                </element>
                <element name = "effective" minOccurs = "0">
                 <simpleType>
                   <restriction base = "xs:dateTime">
                     <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                   </restriction>
                 </simpleType>
                </element>
                <element name = "onset"  minOccurs = "0">
                 <simpleType>
                   <restriction base = "xs:dateTime">
                     <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                   </restriction>
                 </simpleType>
                </element>
                <element name = "expires"  minOccurs = "0">
                 <simpleType>
                   <restriction base = "xs:dateTime">
                     <pattern value = "\d\d\d\d-\d\d-\d\dT\d\d:\d\d:\d\d[-,+]\d\d:\d\d"/>
                   </restriction>
                 </simpleType>
                </element>
                <element name = "senderName" type = "xs:string" minOccurs = "0"/>
                <element name = "headline" type = "xs:string" minOccurs = "0"/>
                <element name = "description" type = "xs:string" minOccurs = "0"/>
                <element name = "instruction" type = "xs:string" minOccurs = "0"/>
                <element name = "web" type = "xs:anyURI" minOccurs = "0"/>
                <element name = "contact" type = "xs:string" minOccurs = "0"/>
                <element name = "parameter" minOccurs = "0" maxOccurs = "unbounded">
                  <complexType>
                    <sequence>
                      <element ref = "cap:valueName"/>
                      <element ref = "cap:value"/>
                    </sequence>
                  </complexType>
                </element>
                <element name = "resource" minOccurs = "0" maxOccurs = "unbounded">
                  <complexType>
                    <sequence>
                      <element name = "Foto del hecho" type = "xs:string"/>
                      <element name = "mimeType" type = "xs:string"/>
                      <element name = "size" type = "xs:integer" minOccurs = "0"/>
                      <element name = "uri" type = "xs:anyURI" minOccurs = "0"/>
                      <element name = "derefUri" type = "xs:string" minOccurs = "0"/>
                      <element name = "digest" type = "xs:string" minOccurs = "0"/>
                    </sequence>
                  </complexType>
                </element>
                <element name = "area" minOccurs = "0" maxOccurs = "unbounded">
                  <complexType>
                    <sequence>
                      <element name = "areaDesc" type = "xs:string"/>
                      <element name = "polygon" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
                      <element name = "circle" type = "xs:string" minOccurs = "0" maxOccurs = "unbounded"/>
                      <element name = "geocode" minOccurs = "0" maxOccurs = "unbounded">
                        <complexType>
                          <sequence>
                            <element ref = "cap:valueName"/>
                            <element ref = "cap:value"/>
                          </sequence>
                        </complexType>
                      </element>
                      <element name = "altitude" type = "xs:decimal" minOccurs = "0"/>
                      <element name = "ceiling" type = "xs:decimal" minOccurs = "0"/>
                    </sequence>
```

```
                </complexType>
              </element>
            </sequence>
          </complexType>
        </element>
        <any minOccurs = "0" maxOccurs = "unbounded" namespace = "http://www.w3.org/2000/09/xmldsig#"
processContents = "lax"/>

      </sequence>
    </complexType>
  </element>
  <element name = "valueName" type = "xs:string"/>
  <element name = "value" type = "xs:string"/>
</schema>
```

9.7 CAD con Sistemas de Gestión de Flota

La Gestión de Flota (SGF) cobra cada vez más importancia por los tiempos que vivimos mientras redactamos este documento: Elevado coste de los combustibles o fuentes de energía para los vehículos, y falta de material de repuesto para los mismos. Su empleo en los servicios de emergencia es corriente (SEM, Bomberos, …)

Relación entre el CAD y el SGF: Los CAD o SGP gestionan los vehículos desde el punto de vista de la operación, y el SGF ayuda a gestionar su ciclo de vida. Para que un CAD pueda despachar un vehículo, este debe estar operativo, en las condiciones requeridas. No tiene sentido asignar un vehículo a un incidente si no tiene combustible suficiente, o si falta algún elemento de su configuración.

Esto es fácilmente comparable con los sistemas de nóminas: Un CAD, aunque sabe cuantas horas al mes ha realizado un agente, no va a generar la nómina y proceder al pago de su salario. Por el mismo motivo, un CAD necesita saber cuando finalizan los turnos de los tripulantes, pero no va a gestionar los cuadrantes de servicios y otras cuestiones relacionadas, puesto que existen sistemas de RRHH capaces de realizar estas funciones.

Que el fabricante del CAD se empeñe en gestionar la planificación de los mantenimientos de los vehículos, o de supervisar si un conductor gasta más o menos gasolina, es pretencioso y da pistas sobre el talante de los directivos de esas compañías cuando su CAD no está siquiera a la altura debida. Si la empresa fabricante es seria, y dispone de recursos, lo ideal sería que su “suite” estuviera diseñada de manera modular, pudiendo permitir al cliente elegir otros componentes de terceros para lograr la solución buscada. Para encontrar soluciones CAD abiertas tenemos que irnos a los grandes fabricantes tipo Telefónica, Atos, Emeres, Hexagon, Motorola, CentralSquare,etc.

10 Conclusiones

A modo de resumen se podrían enunciar las siguientes máximas justificadas a lo largo de este documento:

1. La integración de los sistemas de información en el sector de las emergencias debe suceder mediante el empleo de lenguajes o protocolos de comunicación estándares, abiertos. Mediante webservices diseñados para comunicaciones asíncronas, e incluso redundantes a través de medios de comunicación alternativos para asegurar la entrega.
2. Deben proscribirse integraciones realizadas contra las bases de datos de los otros sistemas, o mediante las API, porque obligan al pago de mantenimientos y licencias, y en caso de reemplazar alguno de los dos sistemas implica volver a pagar por un nuevo conector “idéntico” al ya adquirido. Además estas integraciones generan puntos de fallo únicos que comprometerán al sistema global.
3. EDXL existe desde 2003, y es el recomendado por las principales asociaciones y organismos de emergencias, por lo que está fuera de todo cuestionamiento, y su desconocimiento solo puede significar que esa empresa no es el socio adecuado para un servicio de emergencias.
4. Divide y vencerás: No solamente el cliente tiene siempre razón, sino que la industria debe mostrar absoluto respeto por su función social, y facilitarle la mejor solución aunque no sea toda del mismo proveedor. Cuando un proveedor deja a una agencia de policía sin respuesta para poder integrar lo que esta considere oportuno, ya sea por incompetencia, falta de recursos, o incluso desprecio, debería ser señalada y la comunidad de usuarios advertida para que nadie volviera a exponerse a situaciones similares.
5. RAMS: Los criterios de mantenibilidad, disponibilidad, confiabilidad y seguridad son de vital aplicación para estos sistemas y sus integraciones o interoperabilidad. Los servicios de gestión de emergencia son de “Misión Crítica”, por lo que esta característica debe ser cumplida por sus sistemas TIC, y las integraciones y sistemas de interoperabilidad. El empleo de protocolos abiertos de comunicaciones permite cumplir estos criterios. No así integraciones mediante desarrollos a medida.
6. Zapatero a tus zapatos: Los sistemas COTS disponibles permiten construir soluciones óptimas aprovechando lo mejor de cada uno de estos productos. Esta soluciones, si son interoperables mediante protocolos estándares, abiertos, permiten construir sistemas ajustados a las necesidades de cada agencia, de sus peculiaridades y de sus presupuestos.
7. El cliente no solo tiene la razón sino el mando: Los sistemas TIC empleados por la agencia sirven para salvar vidas, pero si fallan pueden ocasionar muertes. Por este motivo, los requisitos de las agencias para con sus sistemas de información no pueden ser soslayadas, evadidas ni ignoradas. Por ejemplo, en EE:UU., es el FBI quien dicta los requisitos mínimos de un CAD o RMS, requisitos detallados de manera exhaustiva, incluso llegando a definir los campos de cada tipo de dato gestionado por estos sistemas.

8. No hay clientes pequeños ni grandes en el mundo de la Seguridad, de las Emergencias, y por lo tanto no tiene sentido que las licencias ofrecidas a un pequeño municipio carezcan de las funcionalidades requeridas por una gran ciudad. Es escandaloso que se prive a una policía local de integración con su Padrón o Registro de Entrada por cuestiones particulares del proveedor. En ocasiones se debe a que el esfuerzo de integrar el CAD con el Padrón tiene un coste en jornadas/programador imposibles de financiar por el cliente, ni de proporcionar el propio fabricante. Este problema desaparecería si los clientes obligaran a los proveedores a usar sistemas abiertos conforme a su definición explícita: Un sistema informático que proporciona alguna combinación de interoperabilidad, portabilidad y uso de estándares abiertos.
9. Necesidad de Saber: Este criterio es el empleado a la hora de clasificar materias que no son de dominio público. Los criterios para discernir si una policía local puede acceder o no a conocer los expedientes sancionadores de vehículos de otro ayuntamiento, o incluso el Padrón, pueden ser implementados fácilmente sobre una plataforma de interoperabilidad. El cumplimiento de la Ley obliga a los sistemas TIC, pero como las Leyes cambian o evolucionan, los sistemas TIC deben diseñarse para incorporar estos cambios legislativos que faciliten o impidan compartir datos. No tiene sentido en estos tiempos mantener los permisos de accesos a la información mediante procesos burocráticos manuales.
10. Es más barato, seguro, eficiente, mantenible, etc. y elegante un ecosistema de aplicaciones capaces de hablar mediante protocolos abiertos y estandarizados, que no uno donde unas no se hablan con otras, o lo hacen con métodos propietarios, o incluso donde se meten mano sin consentimiento previo (acceso a las bases de datos del otro sistema).
11. Reemplazar sin traumas: Gracias al establecimiento de criterios de interoperabilidad, de integración entre aplicaciones basadas en protocolos de comunicación estándares, cuando una aplicación se quiere reemplazar por otra más conveniente al cliente, esto puede hacerse sin afectar al sistema global.